PATENT ABSTRACTS OF JAPAN

(8)

(11)Publication number : 2004-318478
(43)Date of publication of application : 11.11.2004

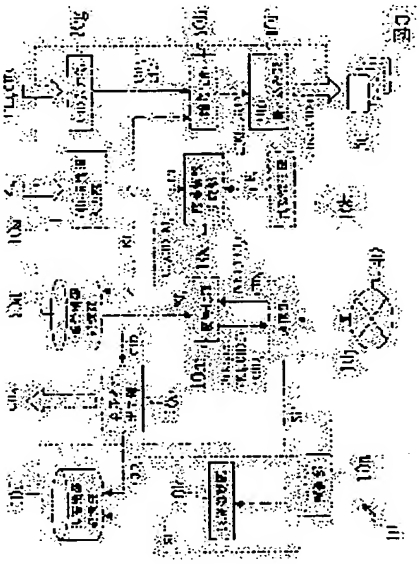
(51)Int.Cl. G06K 17/00
H04L 9/32

(21)Application number : 2003-111342
(22)Date of filing : 16.04.2003

(71)Applicant : NIPPON TELEGR & TELEPH CORP <NTT>
(72)Inventor : KOMURO TOMOYUKI
KINOSHITA SHINGO
HOSHINO FUMISATO
FUJIMURA AKIKO

(54) RF TAG ISSUING DEVICE, RF TAG UTILIZING DEVICE, METHOD FOR UTILIZING RF TAG, AND PROGRAM

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the forgery of an RF tag by enhancing the safety of UID stored in the RF tag.
SOLUTION: The UID inputting part 10g of an RF tag issuing device 10 accepts the input of UID to be stored in a non-contact type radio frequency tag 50. The inputted UID is converted into encrypted UID (E(Kli, UIDj)) by an encrypting part 10h. This encrypted UID (E(Kli, UIDj)) is written in the non-contact type radio frequency tag 50 by a UID writing part 10i. The radio frequency tag 50 in which the encrypted UID (E(Kli, UIDj)) is written in this way is distributed to a user. The encrypted UID (E(Kli, UIDj)) stored in the radio frequency tag 50 is decoded by an RF tag using device which the user uses.



LEGAL STATUS

[Date of request for examination] 26.03.2004
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number]
[Date of registration]
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of rejection]
[Date of extinction of right]

(19)日本国特許庁(JP)　(12)公開特許公報(A)　(11)特許出願公開番号
特開2004-318478
(P2004-318478A)
(43)公開日　平成16年11月11日(2004.11.11)

(51)Int.Cl.[7]	F I		テーマコード（参考）
G06K 17/00	G06K 17/00	S	5B058
H04L 9/32	G06K 17/00	F	5J104
	H04L 9/00	673C	
	H04L 9/00	673E	

審査請求 有　請求項の数 11　OL　（全 36 頁）

(21)出願番号　特願2003-111342(P2003-111342)
(22)出願日　平成15年4月16日(2003.4.16)

(71)出願人　000004226
日本電信電話株式会社
東京都千代田区大手町二丁目３番１号
(74)代理人　100066153
弁理士　草野　卓
(74)代理人　100100642
弁理士　稲垣　稔
(72)発明者　小室　智之
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内
(72)発明者　木下　真吾
東京都千代田区大手町二丁目３番１号　日本電信電話株式会社内

最終頁に続く

(54)【発明の名称】ＲＦタグ発行装置、ＲＦタグ利用装置、ＲＦタグの利用方法、及びプログラム

(57)【要約】
【課題】ＲＦタグに格納されたＵＩＤの安全性を向上させ、その偽造を防止する。
【解決手段】ＲＦタグ発行装置１０のＵＩＤ入力部１０ｇにおいて、非接触型のＲＦタグ５０に格納するＵＩＤの入力を受け付け、暗号化部１０ｈにおいて、入力されたＵＩＤを、暗号化ＵＩＤ（$E(KI_i, UID_j)$）に変換し、ＵＩＤ書き込み部１０ｉにおいて、この暗号化ＵＩＤ（$E(KI_i, UID_j)$）を、非接触型のＲＦタグ５０に書き込む。このように暗号化ＵＩＤ（$E(KI_i, UID_j)$）が書き込まれたＲＦタグ５０は利用者に配布され、利用者が使用するＲＦタグ利用装置において、ＲＦタグ５０に格納されている暗号化ＵＩＤ（$E(KI_i, UID_j)$）が復号される。
【選択図】　図３

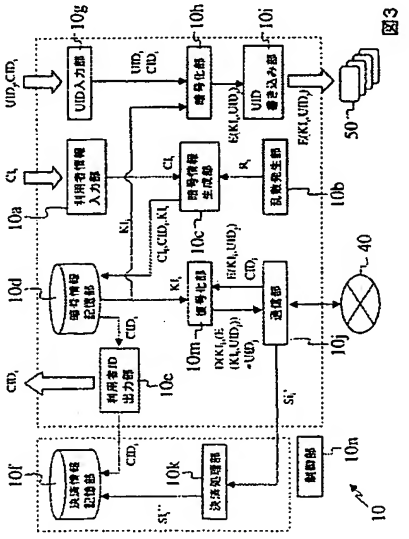


図3

【特許請求の範囲】
【請求項１】
非接触型ＲＦタグを発行するＲＦタグ発行装置において、
上記非接触型ＲＦタグに格納する固有ＩＤ情報の入力を受け付ける固有ＩＤ情報入力手段と、
上記固有ＩＤ情報入力手段において入力された上記固有ＩＤ情報を、所定の情報を用いなければ読解が困難な情報（以下、「変換固有ＩＤ情報」という。）に変換する固有ＩＤ情報変換手段と、
上記固有ＩＤ情報変換手段において変換された上記変換固有ＩＤ情報を、上記非接触型ＲＦタグに書き込む変換固有ＩＤ情報書き込み手段と、
を有することを特徴とするＲＦタグ発行装置。
【請求項２】
前記固有ＩＤ情報入力手段は、
複数の前記固有ＩＤ情報の入力を受け付ける手段であり、
前記固有ＩＤ情報変換手段は、
上記固有ＩＤ情報入力手段において入力された複数の上記固有ＩＤ情報の少なくとも一部を、入力された他の上記固有ＩＤ情報と異なる方法によって、前記変換固有ＩＤ情報に変換する手段であること、
を特徴とする請求項１記載のＲＦタグ発行装置。
【請求項３】
前記変換固有ＩＤ情報を読解可能とするために用いる復元情報に関連付けた復元ＩＤ情報を、前記非接触型ＲＦタグに書き込む、復元ＩＤ情報書き込み手段を、さらに有すること
を特徴とする請求項１或いは２の何れかに記載のＲＦタグ発行装置。
【請求項４】
前記変換固有ＩＤ情報の入力を受け付ける変換固有ＩＤ情報入力手段と、
上記変換固有ＩＤ情報入力手段において入力された上記変換固有ＩＤ情報を、読解可能な情報（以下、「復元固有ＩＤ情報」という。）に変換する固有ＩＤ情報復元手段と、
上記固有ＩＤ情報復元手段において変換された上記復元固有ＩＤ情報を出力する復元固有ＩＤ情報出力手段と、
をさらに有すること、
を特徴とする請求項１から３の何れかに記載のＲＦタグ発行装置。
【請求項５】
前記固有ＩＤ情報の改ざんを防止するための改ざん防止情報を生成する改ざん防止情報生成手段と、
上記改ざん防止情報生成手段において生成された上記改ざん防止情報を前記非接触型ＲＦタグに書き込む、改ざん防止情報書き込み手段とを、さらに有すること、
を特徴とする請求項１から４の何れかに記載のＲＦタグ発行装置。
【請求項６】
非接触型ＲＦタグの利用に用いるＲＦタグ利用装置において、
変換固有ＩＤ情報を読解可能とするために用いる復元情報が、復元ＩＤ情報に対応付けられて格納された復元情報格納手段と、
上記非接触型ＲＦタグから、上記復元ＩＤ情報を読み取る復元ＩＤ情報読み取り手段と、
上記復元ＩＤ情報読み取り手段によって読み取られた上記復元ＩＤ情報を用い、上記復元情報格納手段から、この復元ＩＤ情報に対応する上記復元情報を抽出する復元情報抽出手段と、
上記非接触型ＲＦタグから、上記変換固有ＩＤ情報を読み取る変換固有ＩＤ情報読み取り手段と、
上記復元情報抽出手段によって抽出された上記復元情報を用い、上記変換固有ＩＤ情報読み取り手段によって読み取られた上記変換固有ＩＤ情報を読解可能なように変換する固有

ＩＤ情報復元手段と、
を有することを特徴とするＲＦタグ利用装置。
【請求項７】
非接触型ＲＦタグの利用に用いるＲＦタグ利用装置において、
所定の情報を用いなければ読解が困難な変換固有ＩＤ情報を、上記非接触型ＲＦタグから読み取る変換固有ＩＤ情報読み取り手段と、
上記変換固有ＩＤ情報読み取り手段によって読み取られた上記変換固有ＩＤ情報を出力する変換固有ＩＤ情報出力手段と、
上記変換固有ＩＤ情報が読解可能に変換された復元固有ＩＤ情報の入力を受け付ける復元固有ＩＤ情報入力手段と、
を有することを特徴とするＲＦタグ利用装置。
【請求項８】
前記非接触型ＲＦタグから復元ＩＤ情報を読み取る復元ＩＤ情報読み取り手段を、さらに有し、
前記変換固有ＩＤ情報出力手段は、
上記復元ＩＤ情報読み取り手段によって読み取られた上記復元ＩＤ情報によって特定されるアドレスを指定して、前記変換固有ＩＤ情報を出力する手段であること、
を特徴とする請求項７記載のＲＦタグ利用装置。
【請求項９】
非接触型のＲＦタグの利用方法において、
ＲＦタグ発行装置によって、
上記非接触型ＲＦタグに格納する固有ＩＤ情報の入力を受け付け、
入力された上記固有ＩＤ情報を、所定の情報を用いなければ読解が困難な情報（以下、「変換固有ＩＤ情報」という。）に変換し、
変換された上記変換固有ＩＤ情報を、上記非接触型ＲＦタグに書き込み、
ＲＦタグ利用装置によって、
上記非接触型ＲＦタグから、上記変換固有ＩＤ情報を読み取り、
読み取った上記変換固有ＩＤ情報を出力し、
上記ＲＦタグ発行装置によって、
上記変換固有ＩＤ情報の入力を受け、
入力された上記変換固有ＩＤ情報を、読解可能な情報（以下、「復元固有ＩＤ情報」という。）に変換し、
上記復元固有ＩＤ情報を出力し、
上記ＲＦタグ利用装置によって、
上記復元固有ＩＤ情報の入力を受け付けること、
を特徴とするＲＦタグの利用方法。
【請求項１０】
請求項１から５の何れかに記載されたＲＦタグ発行装置としてコンピュータを機能させるためのプログラム。
【請求項１１】
請求項６から８の何れかに記載されたＲＦタグ利用装置としてコンピュータを機能させるためのプログラム。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】
この発明は、非接触型ＲＦタグを発行するＲＦタグ発行装置、非接触型ＲＦタグの利用に用いるＲＦタグ利用装置、このＲＦタグの利用方法、及びそれらの機能をコンピュータに実行させるためのプログラムに関し、特に、取り扱う情報の安全性の向上を図ったＲＦタグ発行装置、ＲＦタグ利用装置、ＲＦタグの利用方法、及びプログラムに関する。
【０００２】

【従来の技術】
近年、ＲＦＩＤ（Ｒａｄｉｏ Ｆｒｅｑｕｅｎｃｙ ＩＤｅｎｔｉｆｉｃａｔｉｏｎ：電波方式認識）の導入が様々な分野で進んでいる（例えば、非参照文献１参照。）。ＲＦＩＤは、「ＲＦタグ」と呼ばれる小型の情報記録媒体と、「リーダー」と呼ばれる質問器との間で非接触の情報交信を行う技術であり、人の出入りが激しい店舗での万引き防止等のセキュリティ目的の他、商品を取り出さずに検品ができるという利点から、倉庫・運送等の物流管理においても特に有用な技術である。
このＲＦＩＤに使用されるＲＦタグは、非接触ＩＣチップを用いた記録媒体及びアンテナが埋め込まれたプレート（タグ）であり、この記録媒体には「ＵＩＤ：Ｕｎｉｑｕｅ ＩＤｅｎｔｉｆｙ」と呼ばれる各用途に応じた固有値が書き込まれている。通常、このＲＦタグは、衣類や電荷製品等の商品に取り付けられて使用され、このＲＦタグが取り付けられた商品の商品識別番号・商品固体番号等の情報は、そのＲＦタグに格納されたＵＩＤに関連付けて外部のデータベースに保管される。そして、店員等の利用者は、リーダーを用いてＲＦタグからＵＩＤを読み取り、読み取ったＵＩＤをこのデータベースの情報と照合することにより、そのＲＦタグが取り付けられている商品の商品識別番号・商品固体番号等を知ることができる。
【０００３】
【非特許文献１】
Ａｕｔｏ－ＩＤ Ｃｅｎｔｅｒ、”Ａｂｏｕｔ ｔｈｅ ｔｅｃｈｎｏｌｏｇｙ”、［ｏｎｌｉｎｅ］、［平成１５年４月９日検索］、インターネット＜ｈｔｔｐ：／／ｗｗｗ．ａｕｔｏＩＤｃｅｎｔｅｒ．ｏｒｇ／ａｂｏｕｔｔｈｅｃｅｎｔｅｒ．ａｓｐ＞
【０００４】
【発明が解決しようとする課題】
しかし、従来のＲＦタグでは、格納されたＵＩＤの安全性が十分ではないという問題点がある。
つまり、ＲＦタグは、商品とともに流通過程を転々とし、商品が消費者の手に渡った後もその商品と一体に存在する場合がある。そして、このＲＦタグに格納されたＵＩＤは、それを読み取るリーダーを有し、このＵＩＤにアクセスするプロトコルを知っているものであれば、誰でもその内容を読み取ることができる。従って、例えば、甲が乙の所持しているＲＦタグ付の商品を遠隔から読み取り、読み取ったＵＩＤと商品との対応を調べることにより、この甲は乙の所持品を容易に知ることができる。そして、このＲＦタグ付の商品がプライベートなものであればあるほど、乙のプライバシーが侵害される可能性が高くなる。
【０００５】
また、従来のＲＦタグでは、それに格納されているＵＩＤを容易に偽造できてしまうという問題点もある。
つまり、ＲＦタグ付の商品の入手者は、上述のように、ＲＦタグに格納されたＵＩＤを容易に読み取ることができ、この読み取ったＵＩＤと商品との対応を調べることにより、特定の商品のＵＩＤを容易に推測できてしまう。これは、ＵＩＤの設定は、ＵＩＤを使用する際の利便性やコストを考慮し、何らかのルールに従って行われることが通常だからである。そのため、例えば、ブランドや流通過程等を偽った商品に、この偽造したＵＩＤを格納したＲＦタグを付すことにより、ＵＩＤの内容までも再現した偽造商品を容易に製造できてしまう。
【０００６】
また、このような点に考慮し、パスワード等の秘密情報を安全に保管する耐タンパー性を備えた記録媒体と、この秘密情報による認証処理等のアクセス制御を行うＩＣチップとをＲＦタグ内に実装したものもあるが、このようなＲＦタグの価格は高く、個々の商品にこのようなＲＦタグを付与することはコストの面から現実的ではない。
この発明はこのような点に鑑みてなされたものであり、格納するＵＩＤの安全性を向上させ、その偽造を防止できる安価なＲＦタグを発行するＲＦタグ発行装置を提供することで

ある。
【０００７】
また、この発明の他の目的は、格納されたＵＩＤの安全性を向上させ、その偽造を防止できる安価なＲＦタグの利用に用いるＲＦタグ利用装置を提供することである。
さらに、この発明の他の目的は、低コストで、ＲＦタグに格納されたＵＩＤの安全性を向上させ、その偽造の防止を可能にするＲＦタグの利用方法を提供することである。
また、この発明の他の目的は、低コストで、ＲＦタグに格納されたＵＩＤの安全性を向上させ、その偽造の防止を可能にする機能をコンピュータに実行させるためのプログラムを提供することである。
【０００８】
【課題を解決するための手段】
この発明では上記課題を解決するために、まず、非接触型ＲＦタグに格納する固有ＩＤ情報（ＵＩＤ）の入力を受け付け、入力された固有ＩＤ情報を、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）に変換する。そして、この変換された変換固有ＩＤ情報を、非接触型のＲＦタグに書き込む。
ここで、このように発行されたＲＦタグの内容を悪意の者が読み取ったとしても、この者が知り得る情報は変換固有ＩＤ情報のみであり、固有ＩＤ情報自体の内容を知ることはできない。これにより、ＲＦタグに格納されたＵＩＤの安全性向上と、その偽造の防止を図ることができる。さらに、ＲＦタグに秘密情報を保持するための構造や、認証処理を行うためのＩＣを必要としないため、ＲＦタグのコストも安い。
【０００９】
また、この発明において、好ましくは、ＩＤ情報の改ざんを防止するための改ざん防止情報を、非接触型ＲＦタグに書き込む。これにより、ＲＦタグの内容が偽造されたとしても、この改ざん防止情報を検証することにより、容易にその偽造を発見することができる。
【００１０】
【発明の実施の形態】
以下、この発明の実施の形態を図面を参照して説明する。
〔第１の実施の形態〕
この形態は、ＲＦタグ発行装置において、ＵＩＤ（Ｕｎｉｑｕｅ　ＩＤｅｎｔｉｆｙ）を共通鍵によって暗号化してＲＦタグに書き込み、ＲＦタグ利用装置からこのＲＦタグ発行装置に対し、暗号化されたＵＩＤの復号を依頼する形態である。なお、この形態で使用する暗号化アルゴリズムは、共通鍵暗号方式であれば、ＤＥＳ等特に制限はなく、ＲＦタグ発行装置、ＲＦタグ利用装置間において、予め取決め・設定しておくものとする。
【００１１】
図１は、この形態におけるＲＦタグ利用システム１の全体を例示した概念図である。
図１に例示するように、この例のＲＦタグ利用システム１は、非接触型のＲＦタグ５０を発行するＲＦタグ発行装置１０、このＲＦタグ５１～５３の利用に用いる複数のＲＦタグ利用装置２１～２３、及び決済処理を行う決済処理サーバ装置３０によって構成され、これらは物理的又は理論的に安全なネットワーク４０によって、相互に通信可能なように構成されている。なお、このＲＦタグ発行装置１０は、例えば、セキュリティサービスを行う会社が運営し、ＲＦタグ利用装置２１～２３は、ＲＦタグを使用する店舗等に配置されるものである。
【００１２】
図２の（ａ）は、図１に例示したＲＦタグ発行装置１０のハードウェア構成を例示したブロック図であり、図２の（ｂ）は、ＲＦタグ利用装置２１のハードウェア構成を例示したブロック図である。
図２の（ａ）に例示するように、この例のＲＦタグ発行装置１０は、ＣＰＵ（Ｃｅｎｔｒａｌ　Ｐｒｏｃｅｓｓｉｎｇ　Ｕｎｉｔ）１１、キーボード等の入力装置１２、液晶ディスプレイ等の出力装置１３、ハードディスク等の外部記憶装置１４、電磁気的な方法により非接触でＲＦタグに情報を書き込む書き込み装置１５、ＲＡＭ（Ｒａｎｄｏｍ　Ａｃｃ

ｅｓｓ Ｍｅｍｏｒｙ）、ＲＯＭ（Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）等の半導体記憶装置１６、ネットワーク４０と通信可能なように接続され、このネットワーク４０を介した通信を可能にする通信制御装置１７、及びこれらを情報のやり取りが可能なように接続するバス１８を有している。

【００１３】

また、図２の（ｂ）に例示するように、この例のＲＦタグ利用装置２１は、ＣＰＵ２０ａ、入力装置２０ｂ、出力装置２０ｃ、外部記憶装置２０ｄ、電磁気的な方法により非接触でＲＦタグから情報を読み取る読み取り装置２０ｅ、半導体記憶装置２０ｆ、ネットワーク４０と通信可能なように接続され、このネットワーク４０を介した通信を可能にする通信制御装置２０ｇ、及びこれらを情報のやり取りが可能なように接続するバス２０ｈを有している。

なお、その他のＲＦタグ利用装置２２、２３のハードウェア構成も、ＲＦタグ利用装置２１と同様であり、また、決済処理サーバ装置３０のハードウェア構成は、ＲＦタグ発行装置１０から書き込み装置１５を除いたものと同様である。

【００１４】

図３は、図２の（ａ）に例示したハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置１０の機能構成の例示であり、図４は、このＲＦタグ発行装置１０の暗号情報記憶部１０ｄに格納される暗号データベース１００１のデータ構成を例示した図であり、図５は、ＲＦタグ５０に格納されるデータの構成を例示した概念図である。また、図６は、図２の（ｂ）に例示したハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置２１の機能構成の例示であり、図７は、このＲＦタグ利用装置２１に格納されるＵＩＤデータベース１００３の構成を例示した概念図である。また、図８の（ａ）及び（ｃ）は、この例のＲＦタグ発行装置１０の処理を説明するためのフローチャートであり、（ｂ）は、この例のＲＦタグ利用装置２１の処理を説明するためのフローチャートである。

【００１５】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置１０及びＲＦタグ利用装置２１の機能構成及び処理について説明を行っていく。なお、ＲＦタグ発行装置１０の制御は制御部１０ｈによって、ＲＦタグ利用装置２１の制御は制御部２１ｇによって行われる。また、他のＲＦタグ利用装置２２、２３の機能構成及び処理は、以下のＲＦタグ利用装置２１のものと同様である。

また、以下においてＥ，Ｄは、それぞれ暗号化関数、復号関数を意味し、Ｅ（ａ，ｂ）は、鍵ａにより暗号化関数Ｅを用いてｂを暗号化する処理を意味し、Ｄ（ａ，ｂ）は、鍵ａにより復号関数Ｄを用いてｂを復号する処理を意味する。

【００１６】

ＲＦタグの発行：

まず、ＲＦタグ発行の前提として、ＲＦタグの利用者（商品販売業者、サービス提供業者等）の登録を行うため、ＲＦタグ発行装置１０の利用者情報入力部１０ａから利用者情報（CI_i）の入力を受け付ける（ステップＳ１）。入力された利用者情報（CI_i）は暗号情報生成部１０ｃに送られ、暗号情報生成部１０ｃは、これに対応する利用者ＩＤ（CID_i）を生成する。また、乱数発生部１０ｂにおいて、ＳＨＡ－１等の一方向性ハッシュ関数を用いて構成される擬似乱数生成アルゴリズム等を用いて（擬似）乱数（R_i）を発生させ、この乱数（R_i）を暗号情報生成部１０ｃに送る。暗号情報生成部１０ｃでは、これらの情報を用い、共通鍵情報（KI_i）を生成し、生成した共通鍵情報（KI_i）と利用者ＩＤ（CID_i）を、利用者情報（CI_i）とともに暗号情報記憶部１０ｄに送り、そこで暗号データベース１００１として記憶させる（ステップＳ２）。

【００１７】

図４の例の場合、この暗号データベース１００１は、利用者ＩＤ（CID_i）１００１ａ、利用者情報（CI_i）１００１ｂ及び共通鍵情報（KI_i）が相互に関連付けられることによって構成され、利用者ＩＤ（CID_i）「ＡＡ１１１１１１」「ＡＡ１１１１１２

」「ＡＡ１１１１１３」「ＡＡ１１１１１４」に対し、共通鍵情報（$ＫＩ_i$）「１２３４」「１３５７」「２４６８」「９８７６」がそれぞれ対応している。なお、このように記録された利用者ＩＤ（$ＣＩＤ_i$）は、利用者ＩＤ出力部１０ｅから出力され、郵送等によって各利用者に安全に通知される。

次に、ＵＩＤ入力部１０ｇにおいて、商品ＩＤ等の所定の情報に関連付けられた$ＵＩＤ_j$及びＲＦタグを発行する利用者の利用者ＩＤ（$ＣＩＤ_i$）の入力を受け付け、それらを暗号化部１０ｈに送る（ステップＳ４）。暗号化部１０ｈでは、受け取った利用者ＩＤ（$ＣＩＤ_i$）に対応する共通鍵情報（$ＫＩ_i$）を、暗号情報記憶部１０ｄの暗号データベース１００１から抽出し、この共通鍵情報（$ＫＩ_i$）を用い、$ＵＩＤ_j$を暗号化（Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））する（ステップＳ５）。

【００１８】

この暗号化された$ＵＩＤ_j$である暗号化ＵＩＤ（Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））は、ＵＩＤ書き込み部１０ｉに送られ、そこで、ＲＦタグ５０の暗号化ＵＩＤ領域５０ａ（図５）に書き込まれる（ステップＳ６）。なお、ＲＦタグ５０のユーザ領域５０ｂは、後の流通過程等において利用者が自由に情報（価格情報、温度管理情報、産地等）を読み書きできる領域である。

ＲＦタグの利用：

上述のように暗号化ＵＩＤが書き込まれたＲＦタグ５１～５３は、各利用者に配布され、利用者はこのＲＦタグ５１～５３を商品等に取り付ける。取り付けられたＲＦタグ５１～５３は、例えば、商品の在庫管理等の際に、ＲＦタグ利用装置２１～２３によって読み取られる。以下、ＲＦタグ５１の利用手順を例にとって説明を行う。

【００１９】

ＲＦタグ５１を利用する店舗等では、まず、このＲＦタグ５１に格納された暗号化ＵＩＤの復号を依頼のための決済入力（クレジットカード番号等）を行う。この決済入力（$ＳＩ_i$）は、ＲＦタグ利用装置２１の決済処理情報入力部２１ｃにおいて受け付けられ（ステップＳ１０）、通信部２１ｄに送られ、そこからネットワーク４０を介し、決済処理を行う決済処理サーバ装置３０に送られる（ステップＳ１１）。

次に、利用者ＩＤ入力部２１ｂにおいて利用者ＩＤ（$ＣＩＤ_i$）の入力を受け付け（ステップＳ１２）、さらに、ＲＦタグ読み取り部２１ａにおいてＲＦタグ５１の暗号化ＵＩＤ（Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））を読み取る（ステップＳ１３）。これらの利用者ＩＤ（$ＣＩＤ_i$）及び暗号化ＵＩＤ（Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））は、それぞれ通信部２１ｄからネットワーク４０を介してＲＦタグ発行装置１０に送信される（ステップＳ１４）。送信されたこれらの情報（$ＣＩＤ_i$, Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））は、ＲＦタグ発行装置１０の通信部１０ｊにおいて受信され（ステップＳ２０）、復号化部１０ｍに送られる。

【００２０】

復号化部１０ｍでは、受け取った利用者ＩＤ（$ＣＩＤ_i$）に対応する共通鍵情報（$ＫＩ_i$）を暗号情報記憶部１０ｄの暗号データベース１００１から抽出し、この共通鍵情報（$ＫＩ_i$）を用いて、暗号化ＵＩＤ（Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））を復号（Ｄ（$ＫＩ_i$, Ｅ（$ＫＩ_i$, $ＵＩＤ_j$））＝$ＵＩＤ_j$）する（ステップＳ２１）。

その後、通信部１０ｊ、ネットワーク４０を介して決済処理サーバ装置３０にアクセスし、そこで決済処理を行った後、この決済処理サーバ装置３０から出力される決済出力情報（$Ｓｉ_i$'）をネットワーク４０を介して通信部１０ｊで受信する。この決済出力情報（$Ｓｉ_i$'）は、さらに決済処理部１０ｋで処理され、その出力情報（$Ｓｉ_i$''）は決済情報記憶部１０ｆに送られて記憶される（ステップＳ２２）。この際、この出力情報（$Ｓｉ_i$''）は、例えば、利用者ＩＤ出力部１０ｅから送られた利用者ＩＤ（$ＣＩＤ_i$）に対応付けて記憶される。

【００２１】

次に、復号化部１０ｍは、復号した$ＵＩＤ_j$を通信部１０ｊに送り、そこからネットワーク４０を介し、ＲＦタグ利用装置２１に、この$ＵＩＤ_j$を送信する（ステップＳ２３）。送信された$ＵＩＤ_j$は、通信部２１ｄによって受信され（ステップＳ１５）、タグ情報抽

出部２１ｅに送られる。ここで、ＵＩＤデータ記憶部２１ｆには、ＵＩＤ（UID_j）１００３ａと商品ＩＤ（PID_k）を対応付けたＵＩＤデータベース１００３が格納されており（この例では、UID_j＝１２３，４５６，７８９，１０１，１０２に対して、PID_k＝ＬＶ０００１，ＬＶ０００２，ＧＲ０００，ＧＲ０００２が対応付けられている（図７）。）、タグ情報抽出部２１ｅは、送られたUID_jに対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部２１ｆから抽出し、出力する（ステップＳ１６）。

【００２２】

このように、この形態のＲＦタグ発行装置１０では、固有ＩＤ情報入力手段であるＵＩＤ入力部１０ｇにおいて、非接触型のＲＦタグ５０に格納する固有ＩＤ情報（ＵＩＤ）の入力を受け付け、固有ＩＤ情報変換手段である暗号化部１０ｈにおいて、入力された固有ＩＤ情報を、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）である暗号化ＵＩＤ（$E(KI_i, UID_j)$）に変換し、変換固有ＩＤ情報書き込み手段であるＵＩＤ書き込み部１０ｉにおいて、この暗号化ＵＩＤ（$E(KI_i, UID_j)$）を、非接触型のＲＦタグ５０に書き込むこととした。

そのため、このように発行されたＲＦタグ５０の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化ＵＩＤ（$E(KI_i, UID_j)$）のみであり、この者はＵＩＤ自体の内容を知ることができない。その結果、ＲＦタグ５０のＵＩＤの内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【００２３】

また、第三者は、ＲＦタグ５０に格納されたＵＩＤの内容を読み取ることができないため、このＵＩＤと商品の対応から特定の商品のＵＩＤを推測することも容易ではない。その結果、ＵＩＤの偽造をも防止することができる。

さらに、暗号化ＵＩＤ（$E(KI_i, UID_j)$）自体は秘密情報でないため、ＲＦタグ５０に秘密情報を保持するための構造や、認証処理を行うためのＩＣを必要とせず、ＲＦタグ５０のコストも安い。

また、この形態のＲＦタグ発行装置１０では、変換固有ＩＤ情報入力手段である通信部１０ｊにおいて、変換固有ＩＤ情報である暗号化ＵＩＤ（$E(KI_i, UID_j)$）の入力を受け付け、固有ＩＤ情報復元手段である復号化部１０ｍにおいて、この暗号化ＵＩＤ（$E(KI_i, UID_j)$）を、読解可能な情報（復元固有ＩＤ情報）であるUID_jに復号（変換）し、復元固有ＩＤ情報出力手段である通信部１０ｊにおいて、安全なネットワーク４０を介して、このUID_jを出力することとした。

【００２４】

さらに、この形態のＲＦタグ利用装置２１では、変換固有ＩＤ情報読み取り手段であるＲＦタグ読み取り部２１ａにおいて、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）である暗号化ＵＩＤ（$E(KI_i, UID_j)$）を非接触型ＲＦタグ５１から読み取り、変換固有ＩＤ情報出力手段である通信部２１ｄにおいて、この暗号化ＵＩＤ（$E(KI_i, UID_j)$）をＲＦタグ発行装置１０に出力し、復元固有ＩＤ情報入力手段である通信部２１ｄにおいて、ＲＦタグ発行装置１０から返送された復元固有ＩＤ情報（変換固有ＩＤ情報が読解可能に変換された情報）であるUID_jの入力を受け付けることとした。

【００２５】

これにより、暗号化ＵＩＤを復号するための鍵情報（KI_i）をＲＦタグ発行装置１１０のみで安全に管理することが可能となり、悪意の第三者に暗号化ＵＩＤ（$E(KI_i, UID_j)$）が復号され、商品所有者のプライバシー侵害やＵＩＤの偽造等が生じるといった事態を効果的に阻止することできる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、利用者ＩＤ（CID_i）を利用者ごとに設定することとしたが、所定の業種ごと、所定の商品ごと、所定の製造日ごとに、この利用者ＩＤ（CID_i）を設定することとしてもよい。

【００２６】

〔第２の実施の形態〕
この形態は、公開鍵暗号方式によってＵＩＤを暗号化し、ＲＦタグに格納する形態である。なお、第１の実施の形態と共通する事項については説明を省略する（以下の他の形態についても同様。）。なお、この形態で使用する暗号化アルゴリズムは、公開鍵暗号方式であれば、ＲＳＡ等特に制限はなく、ＲＦタグ発行装置、ＲＦタグ利用装置間において、予め取決め・設定しておくものとする。
図９は、この形態におけるＲＦタグ利用システム１０１の全体を例示した概念図である。
【００２７】
図９に例示するように、この例のＲＦタグ利用システム１０１は、ＲＦタグ１５０を発行するＲＦタグ発行装置１１０、ＲＦタグ１５１～１５３の利用に用いるＲＦタグ利用装置１２１～１２３、及び公開鍵証明書を発行する認証局装置１３０によって構成され、これらは物理的又は理論的に安全なネットワーク１４０によって、相互に通信可能なように構成されている。
図１０は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置１１０の機能構成の例示であり、図１１は、ＲＦタグ１５０のデータ構成の例示であり、図１２は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置１２１の機能構成の例示である。また、図１３の（ａ）は、ＲＦタグ発行装置１１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置１２１の処理を説明するためのフローチャートである。
【００２８】
以下、これらの図を用いて、本形態におけるＲＦタグ発行装置１１０及びＲＦタグ利用装置１２１の機能構成及び処理について説明を行っていく。なお、ＲＦタグ発行装置１１０の制御は制御部１１５によって、ＲＦタグ利用装置１２１の制御は制御部１２１ｇによって行われる。また、他のＲＦタグ利用装置１２２、１２３の機能構成及び処理は、以下のＲＦタグ利用装置１２１のものと同様である。
ＲＦタグの発行：
まず、ＲＦタグ利用装置１２１のＵＩＤ入力部１２１ａにおいて、UID_jの入力を受け付け、入力されたUID_jを通信部１２１ｃに送る。また、ネットワーク１４０を介して認証局装置１３０から取得し、鍵情報記憶部１２１ｂに記憶されている公開鍵証明書（Ｃｅｒｔ　PK_c（PK_i））を読み出し、通信部１２１ｃに送る。これらの情報が送られた通信部１２１ｃは、これらのUID_j及び公開鍵証明書（Ｃｅｒｔ　PK_c（PK_i））を、ネットワーク１４０を介し、ＲＦタグ発行装置１１０に送る。なお、SK_cは認証局装置１３０の秘密鍵を、PK_iはＲＦタグ利用装置１２１の公開鍵を意味する。
【００２９】
これらの情報が送られたＲＦタグ発行装置１１０は、通信部１１１によって、これら（UID_j，　Ｃｅｒｔ　PK_c（PK_i））を受信する。また、通信部１１１は、ネットワーク１４０を介し、認証局装置１３０から認証局装置１３０の公開鍵PK_cを取得する（ステップＳ３０）。
通信部１１１に受信された公開鍵証明書（Ｃｅｒｔ　PK_c（PK_i））及び認証局装置１３０の公開鍵PK_cは、公開鍵検証部１１２に送られ、この公開鍵検証部１１２は、（Ｖｅｒｉｆｙ　PK_c（Ｃｅｒｔ　PK_c（PK_i））＝ＯＫ　ｏｒ　ＮＧを検証する（ステップＳ３１）。ここで、ＮＧとなれば、公開鍵PK_cを拒否する旨の信号を暗号化部１１３に送って処理を終了し（ステップＳ３２）、ＯＫとなれば、公開鍵PK_cを受諾する旨の信号を暗号化部１１３に送り、暗号化部１１３は、通信部１１１からUID_jと公開鍵PK_iを取得し、この公開鍵PK_iでUID_jを暗号化（Ｅ（PK_i，UID_j））する（ステップＳ３３）。
【００３０】
このように暗号化されたＥ（PK_i，UID_j）（暗号化ＵＩＤ）は、ＵＩＤ書き込み部１１４に送られ、そこでＲＦタグ１５０の暗号化ＵＤＩ領域１５０ａに書き込まれる（ス

テップＳ３４）。そして、このように暗号化ＵＩＤが書き込まれたＲＦタグ１５０は、各利用者に配布される。なお、ユーザ領域１５０ｂの意味については第１の実施の形態と同様である。

ＲＦタグの利用：

発行されたＲＦタグ１５１を取得した利用者は、このＲＦタグ１５１に格納されているＥ（ＰＫ$_i$，ＵＩＤ$_j$）をＲＦタグ読み取り部１２１ｄによって読み取らせる（ステップＳ４０）。ＲＦタグ読み取り部１２１ｄによって読み取られたＥ（ＰＫ$_i$，ＵＩＤ$_j$）は、復号部１２１ｅに送られ、復号部１２１ｅは、鍵情報記憶部１２１ｂに記憶されているＲＦタグ利用装置１２１の秘密鍵ＳＫ$_i$を抽出する。そして、この暗号部１２１ｅは、抽出した秘密鍵ＳＫ$_i$を用いて受け取ったＥ（ＰＫ$_i$，ＵＩＤ$_j$）を復号し（Ｄ（ＳＫ$_i$，Ｅ（ＰＫ$_i$，ＵＩＤ$_j$））し、その結果ＵＩＤ$_j$をタグ情報抽出部１２１ｇに送る（ステップＳ４１）。タグ情報抽出部１２１ｇでは、第１の実施の形態と同様に、送られたＵＩＤ$_j$に対応する商品ＩＤ（ＰＩＤ$_j$）をＵＩＤデータ記憶部１２１ｆから抽出し、出力する（ステップＳ４２）。

【００３１】

このように、この形態のＲＦタグ発行装置１１０では、固有ＩＤ情報入力手段となる通信部１１１において、非接触型のＲＦタグ１５０に格納する固有ＩＤ情報（ＵＩＤ$_j$）の入力を受け、固有ＩＤ情報変換手段である暗号化部１１３において、この入力されたＵＩＤ$_j$を、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）である暗号化ＵＩＤ（Ｅ（ＰＫ$_i$，ＵＩＤ$_j$））に変換し、変換固有ＩＤ情報書き込み手段であるＵＩＤ書き込み部１１４において、この変換された暗号化ＵＩＤ（Ｅ（ＰＫ$_i$，ＵＩＤ$_j$））を、非接触型のＲＦタグ１５０に書き込むこととした。

そのため、ＲＦタグ２５０の情報を読み取り、ＵＩＤとして利用できる主体を、復号に必要な鍵を所有しているものに限定できる。つまり、このように発行されたＲＦタグ１５０の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化ＵＩＤ（Ｅ（ＰＫ$_i$，ＵＩＤ$_j$））のみであり、この者はＵＩＤ自体の内容を知ることができない。その結果、ＲＦタグ１５０のＵＩＤの内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【００３２】

また、第三者は、ＲＦタグ１５０に格納されたＵＩＤの内容を読み取ることができないため、このＵＩＤと商品の対応から特定の商品のＵＩＤを推測することも容易ではない。その結果、ＵＩＤの偽造をも防止することができる。

さらに、暗号化ＵＩＤ（Ｅ（ＰＫ$_i$，ＵＩＤ$_j$））自体は秘密情報でないため、ＲＦタグ１５０に秘密情報を保持するための構造や、認証処理を行うためのＩＣを必要とせず、ＲＦタグ１５０のコストも安い。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、ＲＦタグ利用装置１２１からネットワーク１４０を介して送られたＵＩＤを、通信部１１１によって受信することにより、ＲＦタグ発行装置１１０にＵＩＤを入力することとしたが、ＲＦタグ発行装置１１０に直接ＵＩＤを入力することとしてもよい。

【００３３】

〔第３の実施の形態〕

この形態は、ＵＩＤを所定の乱数を対応つけ、この乱数をＲＦタグに格納する形態である。なお、第１の実施の形態と共通する事項については説明を省略する。

図１４は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置２１０の機能構成の例示であり、図１５は、乱数情報記憶部２１０ｃに格納された乱数情報１０１１のデータ構成を例示した図であり、図１６は、ＲＦタグ２５０のデータ構成の例示であり、図１７は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置２２０の機能構成の例示である。また、図１８の（ａ）（ｃ）は、ＲＦタグ発行装置２１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用

装置２２０の処理を説明するためのフローチャートである。

【００３４】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置２１０及びＲＦタグ利用装置２２０の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第１の実施の形態と同様のものとする。また、ＲＦタグ発行装置２１０の制御は制御部２１０ｊによって、ＲＦタグ利用装置２２０の制御は制御部２２５によって行われる。

ＲＦタグの発行：

まず、ＲＦタグの発行の前提として、ＲＦタグ発行装置２１０の利用者情報入力部２１０ａから利用者情報（CI_i）の入力を受け付ける（ステップＳ５０）。入力された利用者情報（CI_i）は利用者ＩＤ生成部２１０ｂに送られ、利用者ＩＤ生成部２１０ｂは、これに対応する利用者ＩＤ（CID_i）を生成する。生成された利用者ＩＤ（CID_i）は、乱数情報記憶部２１０ｃに送られ、そこで記憶される（ステップＳ５１）。

【００３５】

この記憶された利用者ＩＤ（CID_i）は、利用者ＩＤ出力部２１０ｄによって抽出・出力され（ステップＳ５２）、各利用者に配布される。また、この出力された利用者ＩＤ（CID_i）は、書き込まれるＵＩＤ（UID_j）とともにＵＩＤ入力部２１０ｅから入力され、乱数情報生成部２１０ｆに送られる（ステップＳ５３）。

利用者ＩＤ（CID_i）とＵＩＤ（UID_j）を受け取った乱数情報生成部２１０ｆは、乱数発生部２１０ｆａによって発生させた乱数（R_j）を取得し、これら利用者ＩＤ（CID_i）、ＵＩＤ（UID_j）、及び乱数（R_j）の対応付けを行う。このように対応つけられた利用者ＩＤ（CID_i）、ＵＩＤ（UID_j）、及び乱数（R_j）は、乱数情報記憶部２１０ｃに送られ、そこで記録される（ステップＳ５４）。

【００３６】

ここで、これらの利用者ＩＤ（CID_i）１０１１ａ、ＵＩＤ（UID_j）１０１１ｄ、及び乱数（R_j）１０１１ｃは、例えば、利用者情報（CI_i）１０１１ｂに対応付けられた乱数情報１０１１として格納される（図１５）。図１５の例の場合、利用者ＩＤ「ＡＡ１１１１１１」に対して、乱数「３２１６５４」とＵＩＤ「１２３４５６」の組み合わせ、及び乱数「６５４７８９」とＵＩＤ「２３４５６７」の組み合わせが対応付けられ、利用者ＩＤ「ＡＡ１１１１１２」に対して、乱数「７４１２５８」とＵＩＤ「９８７６５４」の組み合わせが、利用者ＩＤ「ＡＡ１１１１１３」に対して、乱数「３６９８５２」とＵＩＤ「８７４５６３」の組み合わせ、及び乱数「４８７５３２」とＵＩＤ「７４１２３６」の組み合わせが対応付けられている。

【００３７】

その後、乱数情報生成部２１０ｆは、このＵＩＤに対応つけられた乱数（R_j）をＵＩＤ書き込み部２１０ｇに送り、ＵＩＤ書き込み部２１０ｇは、この乱数（R_j）をＲＦタグ２５０の乱数領域２５１に書きこむ（図１６）（ステップＳ５５）。なお、ＲＦタグ２５０のユーザ領域２５２の意味は、第１の実施の形態と同様ある。そして、このように乱数が書き込まれたＲＦタグ２５０は、各利用者に配布される。

ＲＦタグの利用：

発行されたＲＦタグ２５０を取得した利用者は、まず、ＲＦタグ利用装置２２０に自己の利用者ＩＤ（CID_i）を入力する。この利用者ＩＤ（CID_i）は、利用者ＩＤ入力部２２１に入力され、通信部２２３に送られる（ステップＳ６０）。また、利用者は、ＲＦタグ２５０に格納されている乱数（R_j）をＲＦタグ読み取り部２２２によって読み取らせる（ステップＳ４０）。ＲＦタグ読み取り部１２１ｄによって読み取られた乱数（R_j）も通信部２２３に送られ、通信部は、この乱数（R_j）と利用者ＩＤ（CID_i）とをネットワーク２４０を介し、ＲＦタグ発行装置２１０送信する（ステップＳ６２）。

【００３８】

送信された乱数（R_j）と利用者ＩＤ（CID_i）は、、ＲＦタグ発行装置２１０の通信部２１０ｈで受信され復元部２１０ｉに送られる（ステップＳ７０）。復元部２１０ｉで

は、この乱数（R_j）と利用者ＩＤ（CID_i）とに関連付けられているＵＩＤ（UID_j）を乱数情報記憶部２１０ｃの乱数情報１０１１から抽出し、ＵＩＤ（UID_j）の復元を行う（ステップＳ７１）。このように復元されたＵＩＤ（UID_j）は通信部２１０ｈに送られ、そこからネットワーク２４０を通じてＲＦタグ利用装置２２０に送信される（ステップＳ７２）。

送信されたＵＩＤ（UID_j）は、ＲＦタグ利用装置２２０の通信部２２３によって受信され（ステップＳ６３）、タグ情報抽出部２２５に送られる。タグ情報抽出部２２５では、第１の実施の形態と同様、送られたＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）から抽出し、出力する（ステップＳ６４）。

【００３９】

このように、この形態のＲＦタグ発行装置２１０では、固有ＩＤ情報入力手段であるＵＩＤ入力部２１０ｅにおいて、非接触型のＲＦタグ２５０に格納する固有ＩＤ情報（UID_j）の入力を受け、固有ＩＤ情報変換手段である乱数情報生成部２１０ｆにおいて、この入力されたＵＩＤ$_j$を、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）である乱数（R_j）に変換し、変換固有ＩＤ情報書き込み手段であるＵＩＤ書き込み部２１０ｇにおいて、この変換された乱数（R_j）を、非接触型のＲＦタグ２５０に書き込むこととした。

そのため、ＲＦタグ２５０の情報を読み取り、ＵＩＤとして利用できる主体を、ＵＩＤ$_j$と乱数（R_j）との対応関係を知っているものに限定することができる。つまり、このように発行されたＲＦタグ２５０の内容を悪意の者が読み取ったとしても、この者が知り得る情報は乱数（R_j）のみであり、この者はＵＩＤ自体の内容を知ることができない。その結果、ＲＦタグ２５０のＵＩＤの内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

【００４０】

また、第三者は、ＲＦタグ２５０に格納されたＵＩＤの内容を読み取ることができないため、このＵＩＤと商品の対応から特定の商品のＵＩＤを推測することも容易ではない。その結果、ＵＩＤの偽造をも防止することができる。

さらに、乱数（R_j）自体は秘密情報でないため、ＲＦタグ２５０に秘密情報を保持するための構造や、認証処理を行うためのＩＣを必要とせず、ＲＦタグ２５０のコストも安い。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態において、第１の実施の形態と同様な決済処理を付加した構成としてもよい。

【００４１】

〔第４の実施の形態〕

この形態は、ＵＩＤとともにデジタル署名をＲＦタグに格納する形態である。なお、第１の実施の形態と共通する事項については説明を省略する。また、この形態のデジタル署名に使用する暗号化アルゴリズムは、ＲＳＡ等特に制限はなく、ＲＦタグ発行装置、ＲＦタグ利用装置間において、予め取決め・設定しておくものとする。

図１９は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置３１０の機能構成の例示であり、図２０は、ＲＦタグ３５０のデータ構成の例示であり、図２１は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置３２０の機能構成の例示である。また、図２２の（ａ）は、ＲＦタグ発行装置３１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置３２０の処理を説明するためのフローチャートである。

【００４２】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置３１０及びＲＦタグ利用装置３２０の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第１の実施の形態と同様のものとする。また、ＲＦタグ発行装置３１０の制御は制御部３１５によって、ＲＦタグ利用装置３２０の制御は制御部２２６によって

行われる。
ＲＦタグの発行：
まず、ＲＦタグ発行装置３１０のＵＩＤ入力部３１１においてＵＩＤ（UID_j）の入力を受け付け（ステップＳ８１）、入力されたＵＩＤ（UID_j）を署名部３１３に送る。署名部３１３では、鍵情報記憶部３１２に格納されているＲＦタグ発行装置３１０の秘密鍵SK_iを抽出し、この秘密鍵SK_iを用いて署名（Ｓｉｇ　SK_i（UID_j））を生成する（ステップＳ８２）。生成された署名（Ｓｉｇ　SK_i（UID_j））とＵＩＤ（UID_j）はＵＩＤ書き込み部８３に送られ、そこでＲＦタグ３５０のＵＤＩ領域３５１にＵＩＤ（UID_j）が、署名領域３５２に署名（Ｓｉｇ　SK_i（UID_j））が、それぞれ書き込まれる（図２０）（ステップＳ８３）。なお、ユーザ領域３５３の意味は、第１の実施の形態と同様である。そして、このように署名とＵＩＤが書き込まれたＲＦタグ３５０は、各利用者に配布される。
【００４３】
ＲＦタグの利用：
発行されたＲＦタグ３５０を取得した利用者は、このＲＦタグ３５０の署名（Ｓｉｇ　SK_i（UID_j））とＵＩＤ（UID_j）をＲＦタグ利用装置３２０のＲＦタグ読み取り部３２１に読み取らせる（ステップＳ９１）。読み取られた署名（Ｓｉｇ　SK_i（UID_j））とＵＩＤ（UID_j）は署名検証部３２２に送られ、そこで署名の検証が行われる。すなわち、公開鍵記憶部３２３から、そこに記憶しておいたＲＦタグ発行装置３１０の秘密鍵SK_iに対応する公開鍵PK_iを抽出し、Ｖｅｒｉｆｙ　PK_i（Ｅ（SK_i，UID_j））＝ＯＫ　ｏｒ　ＮＧを検証する（ステップＳ９２）。ここで、ＮＧとなれば、署名を拒否する旨の信号をタグ情報抽出部３２４に送って処理を終了し（ステップＳ９３）、ＯＫとなれば、署名を受諾する旨の信号をタグ情報抽出部３２４に送る。
【００４４】
署名を受諾する旨の信号を受け取ったタグ情報抽出部３２４は、ＲＦタグ読み取り部３２１からＵＩＤ（UID_j）を受け取り、第１の実施の形態と同様に、このＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部３２５から抽出して出力する（ステップＳ９４）。
このように、この形態のＲＦタグ発行装置３１０では、改ざん防止情報生成手段である署名部３１３において、固有ＩＤ情報の改ざんを防止するための改ざん防止情報である署名（Ｓｉｇ　SK_i（UID_j））を生成し、改ざん防止情報書き込み手段に相当するＵＩＤ書き込み部３１４において、この署名（Ｓｉｇ　SK_i（UID_j））を非接触型のＲＦタグ３５０に書き込むこととした。そのため、ＲＦタグ３５０の内容が偽造されたとしても、この署名を検証することにより、容易にその偽造を発見することができる。
【００４５】
なお、この発明は上述の実施の形態に限定されるものではない。
〔第５の実施の形態〕
この形態は、ＵＩＤとともにメッセージ認証子（ＭＡＣ）をＲＦタグに格納する形態である。なお、第１の実施の形態と共通する事項については説明を省略する。なお、この形態で使用するＭＡＣアルゴリズムは、特に制限はなく、ＲＦタグ発行装置、ＲＦタグ利用装置間において、予め取決め・設定しておくものとする。
図２３は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置４１０の機能構成の例示であり、図２４は、ＲＦタグ４５０のデータ構成の例示であり、図２５は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置４２０の機能構成の例示である。また、図２６の（ａ）は、ＲＦタグ発行装置４１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置４２０の処理を説明するためのフローチャートである。
【００４６】
以下、これらの図を用いて、本形態におけるＲＦタグ発行装置４１０及びＲＦタグ利用装

置４２０の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第１の実施の形態と同様のものとする。また、ＲＦタグ発行装置４１０の制御は制御部４１５によって、ＲＦタグ利用装置４２０の制御は制御部４２６によって行われる。

ＲＦタグの発行：

まず、ＲＦタグ発行装置４１０のＵＩＤ入力部４１１においてＵＩＤ（UID_j）の入力を受け付け（ステップＳ１０１）、入力されたＵＩＤ（UID_j）をＭＡＣ演算部４１３に送る。このＭＡＣ演算部４１３では、鍵情報記憶部４１２に格納されているＭＡＣ用の秘密鍵SK_iを抽出し、この秘密鍵SK_iを用いてＭＡＣ（$h(SK_i, UID_j)$）を演算する（ステップＳ１０２）。なお、ｈはＲＦタグ利用装置４２０と共用するハッシュ関数を意味し、ｈ（ａ，ｂ）は、鍵ａを用い、ｂのハッシュ値を求めることを意味する。

【００４７】

生成されたＭＡＣ（$h(SK_i, UID_j)$）及びＵＩＤ（UID_j）は、ＵＩＤ書き込み部４１４に送られ、そこでＲＦタグ４５０のＵＤＩ領域４５１にＵＩＤ（UID_j）が、ＭＡＣ領域４５２にＭＡＣ（$h(SK_i, UID_j)$）が、それぞれ書き込まれる（図２４）（ステップＳ１０３）。なお、ユーザ領域４５３の意味は、第１の実施の形態と同様である。そして、このようにＵＩＤとＭＡＣが書き込まれたＲＦタグ４５０は、各利用者に配布される。

ＲＦタグの利用：

発行されたＲＦタグ３５０を取得した利用者は、このＲＦタグ３５０のＭＡＣ（$h(SK_i, UID_j)$）とＵＩＤ（UID_j）をＲＦタグ利用装置４２０のＲＦタグ読み取り部４２１に読み取らせる（ステップＳ１１１）。読み取られたＭＡＣ（$h(SK_i, UID_j)$）とＵＩＤ（UID_j）はＭＡＣ検証部４２２に送られ、そこでＭＡＣの検証が行われる。すなわち、鍵情報記憶部４２３から、そこに記憶しておいたＭＡＣ用の秘密鍵SK_i'を抽出し、$h(SK_i', UID_j) = h(SK_i, UID_j)$となるか否かを検証する（ステップＳ１１２）。ここで、$h(SK_i', UID_j) = h(SK_i, UID_j)$とならなければ、このＭＡＣを拒否する旨の信号をタグ情報抽出部４２４に送って処理を終了し（ステップＳ１１３）、$h(SK_i', UID_j) = h(SK_i, UID_j)$となれば、ＭＡＣを受諾する旨の信号をタグ情報抽出部４２４に送る。

【００４８】

ＭＡＣを受諾する旨の信号を受け取ったタグ情報抽出部４２４は、ＲＦタグ読み取り部４２１からＵＩＤ（UID_j）を受け取り、第１の実施の形態と同様に、このＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部４２５から抽出して出力する（ステップＳ１１４）。

このように、この形態のＲＦタグ発行装置４１０では、改ざん防止情報生成手段であるＭＡＣ演算部４１３において、固有ＩＤ情報の改ざんを防止するための改ざん防止情報であるＭＡＣ（$h(SK_i, UID_j)$）を生成し、改ざん防止情報書き込み手段に相当するＵＩＤ書き込み部４１４において、このＭＡＣ（$h(SK_i, UID_j)$）を非接触型のＲＦタグ４５０に書き込むこととした。そのため、ＲＦタグ４５０の内容が偽造されたとしても、このＭＡＣを検証することにより、容易にその偽造を発見することができる。

【００４９】

なお、この発明は上述の実施の形態に限定されるものではない。

〔第６の実施の形態〕

この形態は、ＵＩＤを暗号化してＲＦタグに書き込み、さらにこの暗号化されたＵＩＤとともにデジタル署名をＲＦタグに格納する形態である。なお、この形態の例では、公開鍵暗号方式を用いて暗号化、及びデジタル署名の付与を行う。また、使用する暗号化アルゴリズムについては特に制限はないが、ＲＦタグ発行装置、ＲＦタグ利用装置間において、予め取決め・設定しておくものとする。

図２７は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置５１０の機能構成の例示であり、図２８は、

ＲＦタグ５５０のデータ構成の例示であり、図２９は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置５２０の機能構成の例示である。また、図３０の（ａ）及び図３１は、ＲＦタグ発行装置５１０の処理を説明するためのフローチャートであり、図３０の（ｂ）は、ＲＦタグ利用装置５２０の処理を説明するためのフローチャートである。

【００５０】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置５１０及びＲＦタグ利用装置５２０の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第２の実施の形態と同様のものとする。また、ＲＦタグ発行装置５１０の制御は制御部５１７によって、ＲＦタグ利用装置５２０の制御は制御部５２０ｉによって行われる。

ＲＦタグの発行：

まず、ＲＦタグ利用装置５２０のＵＩＤ入力部５２０ａにおいて、UID_jの入力を受け付け、入力されたUID_jを通信部５２０ｃに送る（ステップＳ１２１）。また、ネットワーク５４０を介して認証局装置から取得し、鍵情報記憶部５２０ｂに記憶されている公開鍵証明書（Ｃｅｒｔ　$PK_c(PK_i)$）を読み出し、通信部５２０ｃに送る。これらの情報が送られた通信部５２０ｃは、これらのUID_j及び公開鍵証明書（Ｃｅｒｔ　$PK_c(PK_i)$）を、ネットワーク５４０を介し、ＲＦタグ発行装置５１０に送る（ステップＳ１２２）。なお、SK_cは認証局装置の秘密鍵を、PK_iはＲＦタグ利用装置５２０の公開鍵を意味する。

【００５１】

これらの情報が送られたＲＦタグ発行装置５１０は、通信部５１１によって、これら（UID_j，Ｃｅｒｔ　$PK_c(PK_i)$）を受信する。また、通信部５１１は、ネットワーク５４０を介し、認証局装置から認証局装置の公開鍵PK_cを取得する（ステップＳ１３１）。

通信部５１１に受信された公開鍵証明書（Ｃｅｒｔ　$PK_c(PK_i)$）及び認証局装置の公開鍵PK_cは、公開鍵検証部５１２に送られ、この公開鍵検証部５１２は、（Ｖｅｒｉｆｙ　PK_c（Ｃｅｒｔ　$PK_c(PK_i)$））＝ＯＫ　ｏｒ　ＮＧを検証する（ステップＳ１３２）。ここで、ＮＧとなれば、公開鍵PK_cを拒否する旨の信号を暗号化部５１３に送って処理を終了し（ステップＳ３２）、ＯＫとなれば、公開鍵PK_cを受諾する旨の信号を暗号化部５１３に送り、暗号化部５１３は、通信部５１１からUID_jと公開鍵PK_iを取得し、この公開鍵PK_iでUID_jを暗号化（$E(PK_i, UID_j)$）する（ステップＳ１３４）。

【００５２】

このように暗号化された$E(PK_i, UID_j)$（暗号化ＵＩＤ）は、署名部５１４に送られ、署名部５１４では、鍵情報記憶部５１５に格納されているＲＦタグ発行装置５１０の秘密鍵SK_hを抽出し、この秘密鍵SK_hを用いて署名（Ｓｉｇ　$SK_h(E(PK_i, UID_j))$）を生成する（ステップＳ１３５）。生成された署名（Ｓｉｇ　$SK_h(E(PK_i, UID_j))$）と、暗号化ＵＩＤ（$E(PK_i, UID_j)$）は、ＵＩＤ書き込み部５１６に送られ、そこでＲＦタグ５５０の暗号化ＵＤＩ領域５５１に暗号化ＵＩＤ（$E(PK_i, UID_j)$）が、署名領域５５２に署名（Ｓｉｇ　$SK_h(E(PK_i, UID_j))$）が、それぞれ書き込まれる（図２８）（ステップＳ１３６）。なお、ユーザ領域５５３の意味は、第１の実施の形態と同様である。そして、このように暗号化ＵＩＤ及び署名が書き込まれたＲＦタグ５５０は、各利用者に配布される。

【００５３】

ＲＦタグの利用：

発行されたＲＦタグ５５０を取得した利用者は、このＲＦタグ５５０の署名（Ｓｉｇ　$SK_h(E(PK_i, UID_j))$）と暗号化ＵＩＤ（$E(PK_i, UID_j)$）をＲＦタグ利用装置５２０のＲＦタグ読み取り部５２０ｄに読み取らせる（ステップＳ１４１）。読み取られた署名（Ｓｉｇ　$SK_h(E(PK_i, UID_j))$）と暗号化ＵＩＤ（Ｅ（

PK_i, UID_j)) は署名検証部５２０ｅに送られ、そこで署名の検証が行われる。すなわち、鍵情報記憶部５２０ｂから、そこに記憶しておいたＲＦタグ発行装置５１０の秘密鍵SK_hに対応する公開鍵PK_hを抽出し、Ｖｅｒｉｆｙ PK_h（Ｅ（SK_h, Ｅ（PK_i, UID_j））＝ＯＫ ｏｒ ＮＧを検証する（ステップＳ１４２）。ここで、ＮＧとなれば、署名を拒否する旨の信号を復号部５２０ｆに送って処理を終了し（ステップＳ１４３）、ＯＫとなれば、署名を受諾する旨の信号を復号部５２０ｆに送る。

【００５４】

署名を受諾する旨の信号を受け取った復号部５２０ｆは、ＲＦタグ読み取り部５２０ｄから暗号化ＵＩＤ（Ｅ（PK_i, UID_j））を受け取り、さらに鍵情報記憶部５２０ｂから公開鍵PK_iに対応する秘密鍵SK_iを抽出して、暗号化ＵＩＤ（Ｅ（PK_i, UID_j））を復号（Ｄ（SK_i, Ｅ（PK_i, UID_j））））する（ステップＳ１４４）。その復号結果であるＵＩＤ（UID_j）は、タグ情報抽出部５２０ｇに送られ、タグ情報抽出部５２０ｇは、第１の実施の形態と同様に、このＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部５２０ｈから抽出して出力する（ステップＳ１４５）。

このように、この形態のＲＦタグ発行装置５１０では、固有ＩＤ情報入力手段となる通信部５１１において、非接触型のＲＦタグ５５０に格納する固有ＩＤ情報（UID_j）の入力を受け、固有ＩＤ情報変換手段である暗号化部５１３において、この入力されたUID_jを、所定の情報を用いなければ読解が困難な情報（変換固有ＩＤ情報）である暗号化ＵＩＤ（Ｅ（PK_i, UID_j））に変換し、変換固有ＩＤ情報書き込み手段であるＵＩＤ書き込み部５１４において、この変換された暗号化ＵＩＤ（Ｅ（PK_i, UID_j））を、非接触型のＲＦタグ５５０に書き込むこととした。

【００５５】

そのため、このように発行されたＲＦタグ５５０の内容を悪意の者が読み取ったとしても、この者が知り得る情報は暗号化ＵＩＤ（Ｅ（PK_i, UID_j））のみであり、この者はＵＩＤ自体の内容を知ることができない。その結果、ＲＦタグ５５０のＵＩＤの内容が第三者に読み取られ、商品所有者のプライバシーが侵害されることもない。

また、第三者は、ＲＦタグ５５０に格納されたＵＩＤの内容を読み取ることができないため、このＵＩＤと商品の対応から特定の商品のＵＩＤを推測することも容易ではない。その結果、ＵＩＤの偽造をも防止することができる。

さらに、暗号化ＵＩＤ（Ｅ（PK_i, UID_j））自体は秘密情報でないため、ＲＦタグ５５０に秘密情報を保持するための構造や、認証処理を行うためのＩＣを必要とせず、ＲＦタグ５５０のコストも安い。

【００５６】

また、この形態のＲＦタグ発行装置５１０では、改ざん防止情報生成手段である署名部５１４において、固有ＩＤ情報の改ざんを防止するための改ざん防止情報である署名（Ｓｉｇ SK_h（Ｅ（PK_i, UID_j））））を生成し、改ざん防止情報書き込み手段に相当するＵＩＤ書き込み部５１６において、この署名（Ｓｉｇ SK_h（Ｅ（PK_i, UID_j））））を非接触型のＲＦタグ５５０に書き込むこととした。そのため、ＲＦタグ５５０の内容が偽造されたとしても、この署名を検証することにより、容易にその偽造を発見することができる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、ＲＦタグ利用装置５２０からネットワーク５４０を介して送られたＵＩＤを、通信部５１１によって受信することにより、ＲＦタグ発行装置５１０にＵＩＤを入力することとしたが、ＲＦタグ発行装置５１０に直接ＵＩＤを入力することとしてもよい。また、この形態では公開鍵暗号方式を用いてＵＩＤの暗号化を行い、デジタル署名を付することとしたが、共通鍵暗号方式を用いてＵＩＤの暗号化を行うこととしてもよく、デジタル署名の代わりにＭＡＣによる認証を行う構成としてもよい。さらに、第３の実施の形態のように、ＵＩＤの暗号化の代わりにＵＩＤを乱数に置き換えることとしてもよい。

【００５７】

〔第７の実施の形態〕
この形態は、第２の実施の形態の変形例であり、ＲＦタグに複数の暗号化されたＵＩＤを書き込む形態である。つまり、第２の実施の形態では、ＲＦタグ発行装置において、１つのＲＦタグに対し、１つのＲＦタグ利用装置から１つのＵＩＤと１つの公開鍵を取得し、この公開鍵を用いて暗号化した１つの暗号化ＵＩＤを書き込むこととしていた。これに対し、この形態では、ＲＦタグ発行装置において、１つのＲＦタグに対し、２つのＲＦタグ利用装置からＵＩＤと公開鍵をそれぞれ１つずつ取得し、取得した２つのＵＩＤをそれぞれに対応する公開鍵で暗号化した２つの暗号化ＵＩＤを書き込む形態である。

【００５８】
図３２は、このように暗号化ＵＩＤが格納されたＲＦタグ６００のデータ構成を例示した図である。
この図に例示するように、この暗号化ＵＩＤ領域６０１には、第１のＲＦタグ利用装置から提供されたＵＩＤ$_1$を、この第１のＲＦタグ利用装置の公開鍵ＰＫ$_1$で暗号化した暗号化ＵＩＤ（Ｅ（ＰＫ$_1$，ＵＩＤ$_1$））が格納され、暗号化ＵＩＤ領域６０２には、第２のＲＦタグ利用装置から提供されたＵＩＤ$_2$を、この第２のＲＦタグ利用装置の公開鍵ＰＫ$_2$で暗号化した暗号化ＵＩＤ（Ｅ（ＰＫ$_2$，ＵＩＤ$_2$））が格納される。なお、システム構成及び処理動作については第２の実施の形態と同様であり、ユーザ領域６０３の意味については第１の実施の形態と同様であるため、ここでは説明を省略する。

【００５９】
このように暗号ＵＩＤが格納されたＲＦタグ６００は、例えば、所定の利用者に配布され、そこで所定の商品等に付されて市場を流通する。流通過程においてこのＲＦタグ６００を取得した利用者（仲介業者等）は、自己の秘密鍵を用いて、このＲＦタグ６００に格納されている暗号化ＵＩＤを復号する。この場合、この利用者が復号できるのは、自己が秘密鍵を知っている暗号化ＵＩＤのみであり、その他の暗号化ＵＩＤについては復号できない。従って、この利用者は自己が秘密鍵を知っている暗号化ＵＩＤの内容しか知ることができない。
このように、この形態では、固有ＩＤ情報入力手段（例えば、第２の実施の形態の通信部１１１が相当）において、複数の固有ＩＤ情報（ＵＩＤ）の入力を受け付け、固有ＩＤ情報変換手段（例えば、第２の実施の形態の暗号化部１１３が相当）において、入力された複数のＵＩＤの少なくとも一部を、入力された他のＵＩＤと異なる方法（異なる公開鍵ＰＫ$_1$，ＰＫ$_2$）によって、変換固有ＩＤ情報に変換する（暗号化する）こととした。そのため、利用者は自己が秘密鍵を知っている暗号化ＵＩＤの内容しか知ることができず、流通過程においてＲＦタグが共用される場合であっても、自己の秘密情報が他の利用者に知られてしまうことはない。

【００６０】
なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では、ＵＩＤの暗号化に公開鍵暗号方式を利用したが、共通鍵暗号方式を利用してもよい。また、３以上のＵＩＤを複数の公開鍵を用いて暗号化してＲＦタグ６００に書き込む構成としてもよい。さらに、デジタル署名をＲＦタグ６００に格納する構成としてもよい。

〔第８の実施の形態〕
この形態は、暗号化されたＵＩＤ、その暗号化のアルゴリズム及び鍵を特定するための鍵ＩＤをＲＦタグに書き込むものである。

【００６１】
図３３の（ａ）は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置７１０の機能構成の例示であり、図３３の（ｂ）は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置７２０の機能構成の例示である。また、図３４は、ＲＦタグ発行装置７１０の暗号情報記憶部７１２に格納されるアルゴリズム情報１０２０及び鍵情報１０３０のデータ構成の例示であり、図３５は、ＲＦタグ利用装置７２０の暗号情報記憶部７２３に格納されるアルゴリズム情報１０４０及び鍵情報１０

５０のデータ構成の例示である。さらに、図３６は、ＲＦタグ７５０のデータ構成の例示であり、図３７の（ａ）は、ＲＦタグ発行装置７１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置７２０の処理を説明するためのフローチャートである。

【００６２】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置７１０及びＲＦタグ利用装置７２０の機能構成及び処理について説明を行っていく。なお、システムの全体構成については、例えば、第１の実施の形態と同様のものとする。また、ＲＦタグ発行装置７１０の制御は制御部７１５によって、ＲＦタグ利用装置７２０の制御は制御部７２６によって行われる。

ＲＦタグの発行：

まず、事前処理として、ＲＦタグ発行装置７１０の暗号情報記憶部７１２にアルゴリズム情報１０２０及び鍵情報１０３０が（図３４）、ＲＦタグ利用装置７２０の暗号情報記憶部７２３にアルゴリズム情報１０４０及び鍵情報１０５０が（図３５）、それぞれ格納される。

【００６３】

ここで、この例のアルゴリズム情報１０２０は、ＲＦタグ発行装置７１０においてＵＩＤを暗号化する際に使用する複数の暗号化アルゴリズム（E_m）が、暗号化アルゴリズムＩＤ（EID_m）に対応付けられた情報である。この例では、EID_m＝００１，００３，００３に対し、$E_m=E_1$，E_2，E_3がそれぞれ対応付けられている（図３４）。また、この例の鍵情報１０３０は、ＲＦタグ発行装置７１０においてＵＩＤを暗号化する際に使用する複数の共通鍵（KI_i）が、共通鍵ＩＤ（KID_i）に対応付けられた情報である。この例では、KID_i＝Ｋ００１，Ｋ００３，Ｋ００３に対し、$KI_i=KI_1$，KI_2，KI_3がそれぞれ対応付けられている（図３４）。

【００６４】

さらに、この例のアルゴリズム情報１０４０は、ＲＦタグ利用装置７２０においてＵＩＤを復号する際に使用する複数の復号アルゴリズム（D_m）が、暗号化アルゴリズムＩＤ（EID_m）に対応付けられた情報である。この例では、EID_m＝００１，００３，００３に対し、$D_m=D_1$，D_2，D_3がそれぞれ対応付けられている（図３５）。また、この例の鍵情報１０５０は、ＲＦタグ発行装置７１０の暗号情報記憶部７１２に格納された鍵情報と同じ、複数の共通鍵（KI_i）が、共通鍵ＩＤ（KID_i）に対応付けられた情報である。この例では、KID_i＝Ｋ００１，Ｋ００３，Ｋ００３に対し、$KI_i=KI_1$，KI_2，KI_3がそれぞれ対応付けられている（図３５）。

【００６５】

ＲＦタグの発行を行う場合、まず、ＲＦタグ発行装置７１０のＵＩＤ入力部７１１においてＵＩＤ（UID_j）の入力を受け付け、入力されたＵＩＤ（UID_j）を暗号化部７１３に送る（ステップＳ１５１）。ＵＩＤ（UID_j）を受け取った暗号化部７１３は、暗号情報記憶部７１２から、暗号化に用いる一組の暗号化アルゴリズム（E_m）、暗号化アルゴリズムＩＤ（EID_m）、共通鍵（KI_i）及び共通鍵ＩＤ（KID_i）を抽出し、抽出した暗号化アルゴリズム（E_m）及び共通鍵（KI_i）を用い、ＵＩＤ（UID_j）を暗号化（$E_m(KI_i, UID_j)$）する（ステップＳ１５２）。暗号化されたＵＩＤ（$E_m(KI_i, UID_j)$）、及びその暗号化に使用した抽出した暗号化アルゴリズム（E_m）及び共通鍵（KI_i）に対応する暗号化アルゴリズムＩＤ（EID_m）及び共通鍵ＩＤ（KID_i）はＵＩＤ書き込み部７１４に送られ、ＵＩＤ書き込み部７１４は、それらをＲＦタグ７５０に書き込む（ステップＳ１５３）。図３６の例では、暗号化アルゴリズム領域７５１に暗号化アルゴリズムＩＤ（EID_m）が、鍵ＩＤ領域７５２に共通鍵ＩＤ（KID_i）が、暗号化ＵＩＤ領域７５３に暗号化されたＵＩＤ（$E_m(KI_i, UID_j)$）が、それぞれ格納される。なお、ユーザ領域７５４の意味は第１の実施の形態と同様である。このような書き込みが行われたＲＦタグ７５０は各利用者に配布される。

【００６６】

ＲＦタグの利用：
利用者は、まず、ＲＦタグ利用装置７２０のＲＦタグ読み取り部７２１にＲＦタグ７５０に格納されている暗号化アルゴリズムＩＤ（EID_m）、共通鍵ＩＤ（KID_i）及び暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）を読み取らせる（ステップＳ１６１）。
読み取られたこれらの情報は復号部７２２に送られ、復号部７２２は、受け取った暗号化アルゴリズムＩＤ（EID_m）及び共通鍵ＩＤ（KID_i）にそれぞれ対応付けられている復号アルゴリズム（D_m）及び共通鍵（KI_i）を、暗号情報記憶部７２３に格納されているアルゴリズム情報１０４０及び鍵情報１０５０から抽出する（ステップＳ１６２）。これらを抽出した復号部７２２は、抽出した復号アルゴリズム（D_m）及び共通鍵（KI_i）を用い、受け取った暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）を復号（$D_m(KI_i, E_m(KI_i, UID_j))$）し（ステップＳ１６３）、その復号結果であるＵＩＤ（UID_j）をタグ情報抽出部７２４に送る。
【００６７】
ＵＩＤ（UID_j）を受け取ったタグ情報抽出部７２４は、第１の実施の形態と同様に、このＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部７２５から抽出して出力する（ステップＳ１６４）。
このように、この形態では、ＲＦタグ発行装置７１０のＵＩＤ書き込み部７１４（復元ＩＤ情報書き込み手段に相当）において、暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）（変換固有ＩＤ情報に相当）を読解可能とするために用いる復号アルゴリズム（D_m）及び共通鍵（KI_i）（復元情報に相当）に関連付けた暗号化アルゴリズムＩＤ（EID_m）及び共通鍵ＩＤ（KID_i）（復元ＩＤ情報に相当）を、非接触型のＲＦタグ７５０に書き込むこととした。
【００６８】
これにより、アルゴリズム情報１０２０、１０４０及び鍵情報１０３０、１０５０を、ＲＦタグ発行装置７１０及びＲＦタグ利用装置７２０において保持しておけば、予め、ＲＦタグ５０の発行に用いる暗号化アルゴリズムや鍵を、ＲＦタグ発行装置７１０―ＲＦタグ利用装置７２０間において取決めておかなくても、このＲＦタグ５０の発行・利用を行うことができる。そのため、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にＲＦタグを利用することが可能となる。
また、この形態では、ＲＦタグ利用装置７２０の暗号情報記憶部７２３（復元情報格納手段に相当）に、暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）（変換固有ＩＤ情報に相当）を読解可能とするために用いる復号アルゴリズム（D_m）及び暗号化鍵（KI_i）（復元情報に相当）を、暗号化アルゴリズムＩＤ（EID_m）及び暗号化鍵ＩＤ（KID_i）（復元ＩＤ情報に相当）に対応付けて格納しておき、復元ＩＤ情報読み取り手段であるＲＦタグ読み取り部７２１において、非接触型のＲＦタグ７５０から、暗号化アルゴリズムＩＤ（EID_m）及び暗号化鍵ＩＤ（KID_i）を読み取り、復元情報抽出手段である復号部７２２において、この読み取られた暗号化アルゴリズムＩＤ（EID_m）及び暗号化鍵ＩＤ（KID_i）を用い、暗号情報記憶部７２３から、この暗号化アルゴリズムＩＤ（EID_m）及び暗号化鍵ＩＤ（KID_i）に対応する復号アルゴリズム（D_m）及び暗号化鍵（KI_i）を抽出し、変換固有ＩＤ情報読み取り手段であるＲＦタグ読み取り部７２１において、ＲＦタグ７５０から、暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）を読み取り、固有ＩＤ情報復元手段である復号部７２２において、抽出した復号アルゴリズム（D_m）及び暗号化鍵（KI_i）を用い、暗号化ＵＩＤ（$E_m(KI_i, UID_j)$）を復号（読解可能なように変換）することとした。
【００６９】
これにより、上述のように、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にＲＦタグを利用することが可能となる。
なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態では共

通鍵暗号方式によってＵＩＤを暗号化してＲＦタグ７５０に格納することとしたが、その他の暗号方式や第３の実施の形態のような乱数の置き換えによってＵＩＤを変換し、ＲＦタグ７５０に格納することとしてもよい。

〔第９の実施の形態〕

この形態は、暗号化ＵＩＤとともに、この復号処理当を行う装置へのアクセス情報をＲＦタグに格納するものである。

【００７０】

図３８は、この形態におけるＲＦタグ利用システム８００の全体を例示した概念図である。

図３８に例示するように、この例のＲＦタグ利用システム８００は、非接触型のＲＦタグ８５０を発行するＲＦタグ発行装置８１０、このＲＦタグ８５１～８５３の利用に用いる複数のＲＦタグ利用装置８２１～８２３、及び暗号化ＵＩＤの復号処理等を行う複数のＩＤ管理局装置８３１～８３２によって構成され、ＲＦタグ利用装置８２１～８２３、及びＩＤ管理局装置８３１～８３２は、物理的又は理論的に安全なネットワーク８４０によって、相互に通信可能なように構成されている。

【００７１】

図３９の（ａ）は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置８１０の機能構成の例示であり、図３９の（ｂ）は、図２の（ｂ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ利用装置８２１の機能構成の例示であり、図４０は暗号情報記憶部８１２に格納される暗号情報１０６０のデータ構成の例示であり、図４１は、ＲＦタグ８５０のデータ構成の例示である。また、図４２の（ａ）は、図２の（ａ）と同様なハードウェア構成において所定のプログラムを実行させることによって構成されるＩＤ管理局装置８３１の機能構成の例示であり、（ｂ）は、管理情報記憶部８３１ｃに格納されるＩＤ管理情報１０７０のデータ構成の例示である。さらに、図４３の（ａ）は、ＲＦタグ発行装置８１０の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置８２１及びＩＤ管理局装置８３１の処理を説明するためのフローチャートである。

【００７２】

以下、これらの図を用いて、本形態におけるＲＦタグ発行装置８１０及びＲＦタグ利用装置８２１の機能構成及び処理について説明を行っていく。なお、ここでは、ＲＦタグ利用装置８２１及びＩＤ管理局装置８３１を例にとって説明するが、その構成及び処理は、その他のＲＦタグ利用装置８２２～８２２及びＩＤ管理局装置８３２についても同様とする。また、ＲＦタグ発行装置８１０の制御は制御部８１５によって、ＲＦタグ利用装置８２１の制御は制御部８２１ｃによって、ＩＤ管理局装置８３１の制御は制御局８３１ｄによって行われる。

ＲＦタグの発行：

まず、事前処理として、ＲＦタグ発行装置８１０の暗号情報記憶部８１２に暗号情報１０６０が、ＩＤ管理局装置８３１の管理情報記憶部８３１ｃにＩＤ管理情報１０７０が格納される。

【００７３】

図４０に例示するように、暗号情報１０６０は、ＩＤ管理局装置８３１～８３２にアクセスするためのアドレス等のアクセスＩＤ（AID_i）１０６１、暗号、署名といった処理の種類１０６２、それに使用するアルゴリズム（E_i）１０６３、及び鍵情報（KI_i）１０６４が相互に関連付けられた情報である。この例では、AID_i＝０００１に対して、種類「暗号」、E_i＝ＤＥＳ、KI_i＝０２３４が、AID_i＝０００２に対して、種類「署名」、E_i＝ＲＳＡ、KI_i＝１２３４が、それぞれ関連付けられている。

また、図４２に例示するように、ＩＤ管理情報１０７０は、ＩＤ管理局装置８３１のアクセスＩＤ（AID_i）１０７１、取り扱う処理の種類１０７２、そのアルゴリズム（D_i）１０７３、及び鍵情報（KI_i）１０７４が対応付けられて格納されている。なお、こ

のＩＤ管理情報の内容は、ＩＤ管理局装置８３１～８３２ごとに異なるものとする。

【００７４】

ＲＦタグ８５０の発行を行う場合、まず、ＲＦタグ発行装置８１０のＵＩＤ入力部８１１においてアクセスＩＤ（AID_i）とＵＩＤ（UID_j）の入力を受け付ける（ステップＳ１７１）。入力されたアクセスＩＤ（AID_i）とＵＩＤ（UID_j）は暗号化部８１３に送られ、暗号化部８１３は、このアクセスＩＤ（AID_i）に対応付けられているアルゴリズム（E_i）及び鍵情報（KI_i）を暗号情報記憶部８１２から抽出する。これらを抽出した暗号化部８１３は、受け取ったＵＩＤ（UID_j）に対し、抽出したアルゴリズム（E_i）及び鍵情報（KI_i）を用いた処理を行う。この例ではアクセスＩＤとしてAID_i＝０００１が入力され、ＵＩＤ（UID_j）を、アルゴリズム（E_i）及び鍵情報（KI_i）を用いて暗号化（$E_i(KI_i, UID_j)$）する処理を行うものとする（ステップＳ１７２）。

【００７５】

このように暗号化ＵＩＤ（$E_i(KI_i, UID_j)$）とアクセスＩＤ（AID_i）は、ＵＩＤ書き込む部８１４に送られ、ＵＩＤ書き込む部８１４は、ＲＦタグ８５０のアクセスＩＤ領域にアクセスＩＤ（AID_i）を、暗号化ＵＤＩ領域８５２に暗号化されたＵＩＤ（$E_i(KI_i, UID_j)$）を書き込む（ステップＳ１７３）。そして、このような情報が書き込まれたＲＦタグ８５０は各利用者に配布される。なお、ユーザ領域８５３の意味は第１の実施の形態と同様である。

ＲＦタグの利用：

ＲＦタグ８５１を受け取った利用者は、まず、ＲＦタグ利用装置８２１のＲＦタグ読み取り部８２１ａに、このＲＦタグ８５１に格納された暗号化ＵＩＤ（$E_i(KI_i, UID_j)$）とアクセスＩＤ（AID_i）を読み取らせる（ステップＳ１８１）。読み取られたこれらの情報は、通信部８２１ｂに送られ、通信部８２１ｂは、受け取ったアクセスＩＤ（AID_i）によって特定されるＩＤ管理局装置８３１に、暗号化ＵＩＤ（$E_i(KI_i, UID_j)$）とアクセスＩＤ（AID_i）とを送信する（ステップＳ１８２）。

【００７６】

送信されたこれらの情報は、ネットワーク８４０を介してＩＤ管理局装置８３１に送られ、その通信部８３１ａによって受信される（ステップＳ１８３）。通信部８３１ａは、受信したこれらの情報を復号部８３１ｂに送り、復号部８３１ｂは、このアクセスＩＤ（AID_i）に関連付けられているアルゴリズム（D_i）と鍵情報（KI_i）を管理情報記憶部８３１ｃのＩＤ管理情報１０７０から抽出する。これらを抽出した復号部８３１ｂは、抽出したアルゴリズム（D_i）と鍵情報（KI_i）を用い、受信した暗号化ＵＩＤ（$E_i(KI_i, UID_j)$）を復号（$D_i(KI_i, E_i(KI_i, UID_j))$）する（ステップＳ１８４）。その復号結果（$UID_j$）は、通信部８３１ａに送られ、通信部８３１ａは、この復号結果であるＵＩＤ（UID_j）を、ネットワーク８４０を通じ、元のＲＦタグ利用装置８２１に送信する（ステップＳ１８５）。

【００７７】

送信されたＵＩＤ（UID_j）は、ＲＦタグ利用装置８２１の通信部８２１ｂによって受信され（ステップＳ１８６）、タグ情報抽出部８２１ｃに送られる。そして、このＵＩＤ（UID_j）を受け取ったタグ情報抽出部８２１ｃは、第１の実施の形態と同様に、このＵＩＤ（UID_j）に対応する商品ＩＤ（PID_k）をＵＩＤデータ記憶部８２１ｄから抽出して出力する（ステップＳ１８７）。

このように、この形態のＲＦ利用装置８２１は、復元ＩＤ情報読み取り手段であるＲＦタグ読み取り部８２１ａによって、非接触型のＲＦタグ８５１から復元ＩＤ情報であるアクセスＩＤ（AID_i）を読み取り、変換固有ＩＤ情報出力手段である通信部８２１ｂにおいて、この読み取られたアクセスＩＤ（AID_i）によって特定されるアドレスを指定して、変換固有ＩＤ情報である暗号化ＵＩＤ（$E_i(KI_i, UID_j)$）を出力することとした。

【００７８】

そのため、このアクセスＩＤ（ＡＩＤ$_i$）によって特定されるＩＤ管理局装置８３１に、この暗号化ＵＩＤ（Ｅ$_i$（ＫＩ$_i$，ＵＩＤ$_j$））の復号に必要なアルゴリズム（Ｄ$_i$）と鍵情報（ＫＩ$_i$）をアクセスＩＤ（ＡＩＤ$_i$）に対応付けて格納しておくことにより、このＩＤ管理局装置８３１において、この暗号化ＵＩＤ（Ｅ$_i$（ＫＩ$_i$，ＵＩＤ$_j$））の復号に必要なアルゴリズム（Ｄ$_i$）と鍵情報（ＫＩ$_i$）を導出し、その復号を行うことができる。従って、ＲＦタグ発行者と利用者との間で予め使用するアルゴリズムや鍵情報の合意がなくても、その利用者はＲＦタグを復号することが可能となり、限られたメンバーのみの閉じた環境だけではなく、不特定多数の利用者が使用するようなオープンな環境においても安全にＲＦタグを利用することが可能となる。

【００７９】

また、ヘッダ領域を設けず、通常ＵＩＤが書き込まれる領域をアクセスＩＤ領域８５１とした場合、この形態のタグ構成を通常のＲＦタグフォーマットによって実現することができる。この場合、ＲＦタグのデータ読み込みのために、新たなプログラムを用意する必要がなくなる。

なお、この発明は上述の実施の形態に限定されるものではない。例えば、この形態の説明では、暗号処理に関連付けられたアクセスＩＤ（ＡＩＤ$_i$）が入力された場合を例にとって説明したが、署名処理に関連付けられたアクセスＩＤ（ＡＩＤ$_i$）が入力された場合であっても、その処理は、暗号化が署名生成に変わり、復号が署名検証に変わるのみであって同様である。

【００８０】

また、上述の各実施の形態で説明したＲＦタグのフォーマットは単なる例示であり、これに限定されるものではない。例えば、ユーザ領域のないフォーマット、アクセス制御機能のついたフォーマット等を用いることとしてもよい。

さらに、上述の各実施の形態を組み合わせた構成をとることとしてもよい。

また、上述の各実施の形態では、コンピュータ上で所定のプログラムを実行させることにより、ＲＦタグ発行装置、ＲＦタグ利用装置、決済処理サーバ装置、認証局装置及びＩＤ管理局装置を構成することとしたが、これらの処理内容の少なくとも一部をハードウェア的に実現することとしてもよい。

【００８１】

さらに、上述のように、この形態のＲＦタグ発行装置、ＲＦタグ利用装置、決済処理サーバ装置、認証局装置及びＩＤ管理局装置が有すべき機能の処理内容をプログラムに記述し、このプログラムをコンピュータで実行することにより、これらの処理機能をコンピュータ上で実現することができる。

なお、この処理内容を記述したプログラムは、コンピュータで読み取り可能な記録媒体に記録しておくことができる。コンピュータで読み取り可能な記録媒体としては、例えば、磁気記録装置、光ディスク、光磁気記録媒体、半導体メモリ等どのようなものでもよいが、具体的には、例えば、磁気記録装置として、ハードディスク装置、フレキシブルディスク、磁気テープ等を、光ディスクとして、ＤＶＤ（Ｄｉｇｉｔａｌ Ｖｅｒｓａｔｉｌｅ Ｄｉｓｃ）、ＤＶＤ－ＲＡＭ（Ｒａｎｄｏｍ Ａｃｃｅｓｓ Ｍｅｍｏｒｙ）、ＣＤ－ＲＯＭ（Ｃｏｍｐａｃｔ Ｄｉｓｃ Ｒｅａｄ Ｏｎｌｙ Ｍｅｍｏｒｙ）、ＣＤ－Ｒ（Ｒｅｃｏｒｄａｂｌｅ）／ＲＷ（ＲｅＷｒｉｔａｂｌｅ）等を、光磁気記録媒体として、ＭＯ（Ｍａｇｎｅｔｏ－Ｏｐｔｉｃａｌ ｄｉｓｃ）等を、半導体メモリとしてＥＰＲＯＭ（Ｅｒａｓａｂｌｅ ａｎｄ Ｐｒｏｇｒａｍｍａｂｌｅ ＲＯＭ）等を用いることができる。

【００８２】

また、このプログラムの流通は、例えば、そのプログラムを記録したＤＶＤ、ＣＤ－ＲＯＭ等の可搬型記録媒体を販売、譲渡、貸与等することによって行う。さらに、このプログラムをサーバコンピュータの記憶装置に格納しておき、ネットワークを介して、サーバコンピュータから他のコンピュータにそのプログラムを転送することにより、このプログラムを流通させる構成としてもよい。

このようなプログラムを実行するコンピュータは、例えば、まず、可搬型記録媒体に記録されたプログラムもしくはサーバコンピュータから転送されたプログラムを、一旦、自己の記憶装置に格納する。そして、処理実行時、このコンピュータは、自己の記録媒体に格納されたプログラムを読み取り、読み取ったプログラムに従った処理を実行する。また、このプログラムの別の実行形態として、コンピュータが可搬型記録媒体から直接プログラムを読み取り、そのプログラムに従った処理を実行することとしてもよく、さらに、コンピュータにサーバコンピュータからプログラムが転送されるたびに、逐次、受け取ったプログラムに従った処理を実行することとしてもよい。

【００８３】

【発明の効果】

以上説明したように、この発明では、非接触型ＲＦタグに格納する固有ＩＤ情報の入力を受け付け、入力された固有ＩＤ情報を、所定の情報を用いなければ読解が困難な情報に変換し、この変換された変換固有ＩＤ情報を、非接触型のＲＦタグに書き込むこととしたため、低コストで、ＲＦタグに格納されたＵＩＤの安全性を向上させ、その偽造を防止することが可能となる。

【図面の簡単な説明】

【図１】ＲＦタグ利用システムの全体を例示した概念図。

【図２】（ａ）は、図１に例示したＲＦタグ発行装置のハードウェア構成を例示したブロック図であり、（ｂ）は、ＲＦタグ利用装置のハードウェア構成を例示したブロック図である。

【図３】図２の（ａ）に例示したハードウェア構成において所定のプログラムを実行させることによって構成されるＲＦタグ発行装置の機能構成の例示。

【図４】ＲＦタグ発行装置の暗号情報記憶部に格納される暗号データベースのデータ構成を例示した図。

【図５】ＲＦタグに格納されるデータの構成を例示した概念図。

【図６】ＲＦタグ利用装置の機能構成を例示した図。

【図７】ＲＦタグ利用装置に格納されるＵＩＤデータベースの構成を例示した概念図。

【図８】（ａ）及び（ｃ）は、この例のＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、この例のＲＦタグ利用装置の処理を説明するためのフローチャートである。

【図９】ＲＦタグ利用システムの全体を例示した概念図。

【図１０】ＲＦタグ発行装置の機能構成を例示した図。

【図１１】ＲＦタグのデータ構成を例示した図。

【図１２】ＲＦタグ利用装置の機能構成を例示した図。

【図１３】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。

【図１４】ＲＦタグ発行装置の機能構成を例示した図。

【図１５】乱数情報記憶部に格納された乱数情報のデータ構成を例示した図。

【図１６】ＲＦタグのデータ構成を例示した図。

【図１７】ＲＦタグ利用装置の機能構成を例示した図。

【図１８】（ａ）（ｃ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。

【図１９】ＲＦタグ発行装置の機能構成を例示した図。

【図２０】ＲＦタグのデータ構成を例示した図。

【図２１】ＲＦタグ利用装置の機能構成を例示した図。

【図２２】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。

【図２３】ＲＦタグ発行装置の機能構成を例示した図。

【図２４】ＲＦタグのデータ構成を例示した図。

【図２５】ＲＦタグ利用装置の機能構成を例示した図。

【図２６】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。
【図２７】ＲＦタグ発行装置の機能構成を例示した図。
【図２８】ＲＦタグのデータ構成を例示した図。
【図２９】ＲＦタグ利用装置の機能構成を例示した図。
【図３０】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。
【図３１】ＲＦタグ発行装置の処理を説明するためのフローチャート。
【図３２】ＲＦタグのデータ構成を例示した図。
【図３３】（ａ）は、ＲＦタグ発行装置の機能構成を例示した図であり、（ｂ）は、ＲＦタグ利用装置の機能構成を例示した図である。
【図３４】ＲＦタグ発行装置の暗号情報記憶部に格納されるアルゴリズム情報及び鍵情報のデータ構成を例示した図。
【図３５】ＲＦタグ利用装置の暗号情報記憶部に格納されるアルゴリズム情報及び鍵情報のデータ構成を例示した図。
【図３６】ＲＦタグのデータ構成を例示した図。
【図３７】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置の処理を説明するためのフローチャートである。
【図３８】ＲＦタグ利用システムの全体を例示した概念図。
【図３９】（ａ）は、ＲＦタグ発行装置の機能構成を例示した図であり、（ｂ）は、ＲＦタグ利用装置の機能構成を例示した図。
【図４０】暗号情報記憶部に格納される暗号情報のデータ構成を例示した図。
【図４１】ＲＦタグのデータ構成を例示した図。
【図４２】（ａ）は、ＩＤ管理局装置の機能構成を例示した図であり、（ｂ）は、管理情報記憶部に格納されるＩＤ管理情報のデータ構成を例示した図である。
【図４３】（ａ）は、ＲＦタグ発行装置の処理を説明するためのフローチャートであり、（ｂ）は、ＲＦタグ利用装置及びＩＤ管理局装置の処理を説明するためのフローチャートである。
【符号の説明】
１、１０１、８００　ＲＦタグ利用システム
１０、１１０、２１０、３１０、４１０、５１０、７１０、８１０　ＲＦタグ発行装置
２１～２３、１２１～１２３、２２０、３２０、４２０、５２０、７２０、８２１～８２３　ＲＦタグ利用装置
５０～５３、１５０～１５３、２５０、３５０、４５０、５５０、６００、７５０、８５０～８５３　ＲＦタグ

【図１】

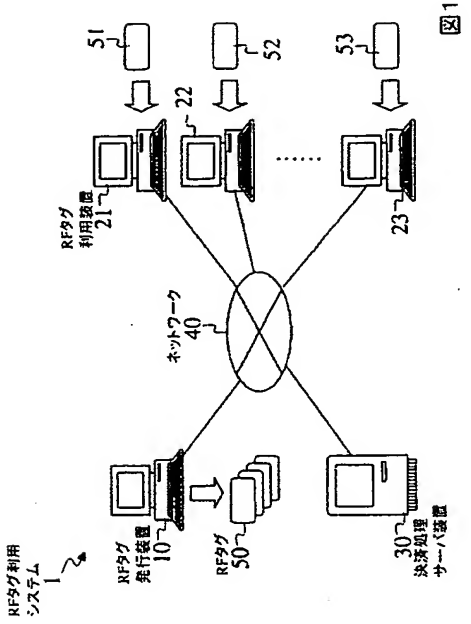


図1

【図２】

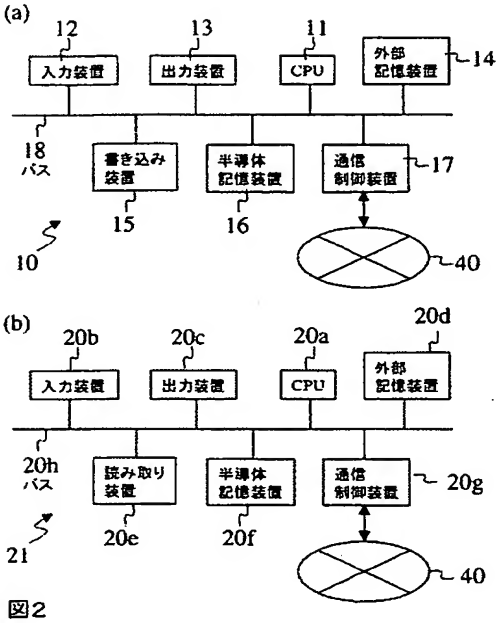


図2

【図３】

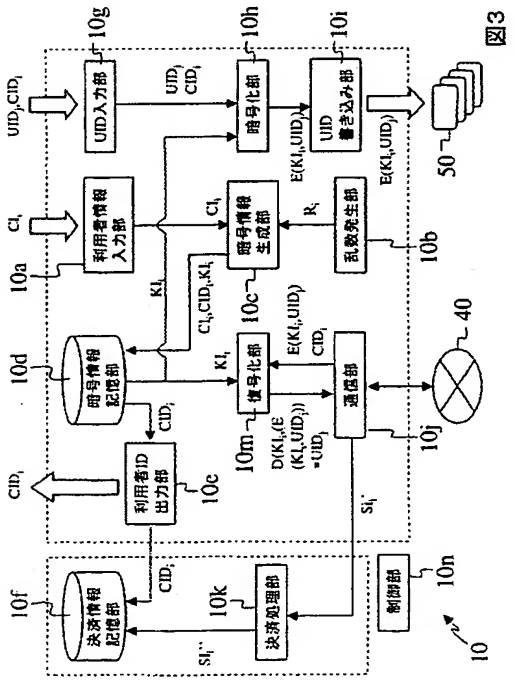


図3

【図４】

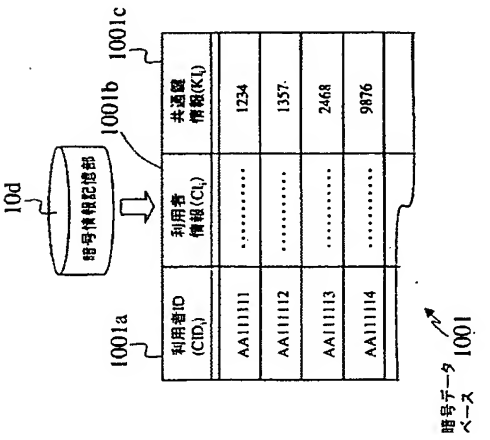


図4

【図５】

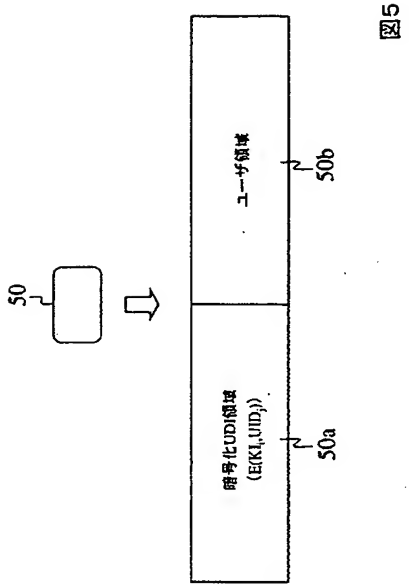


図5

【図６】

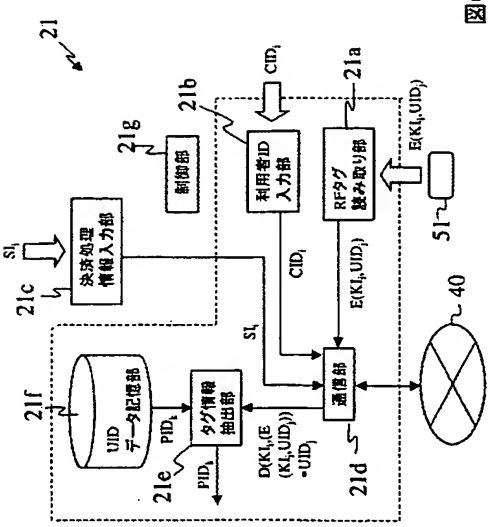


図6

【図７】

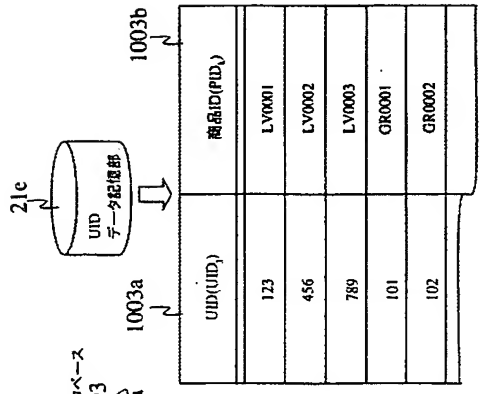


図7

【図８】

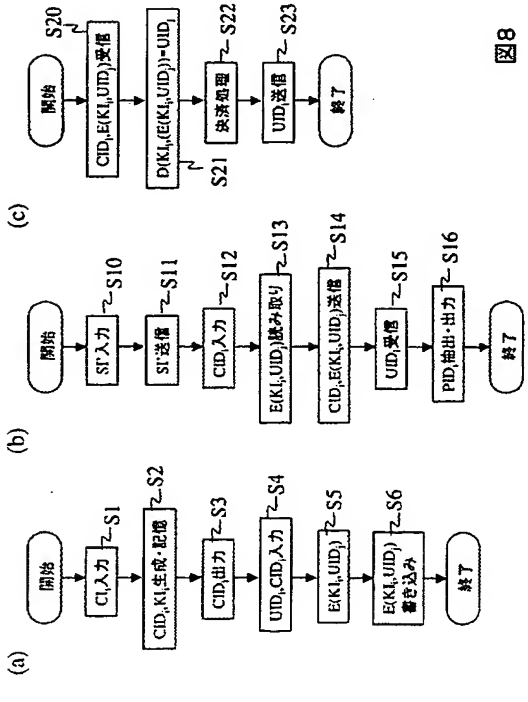


図8

【図９】

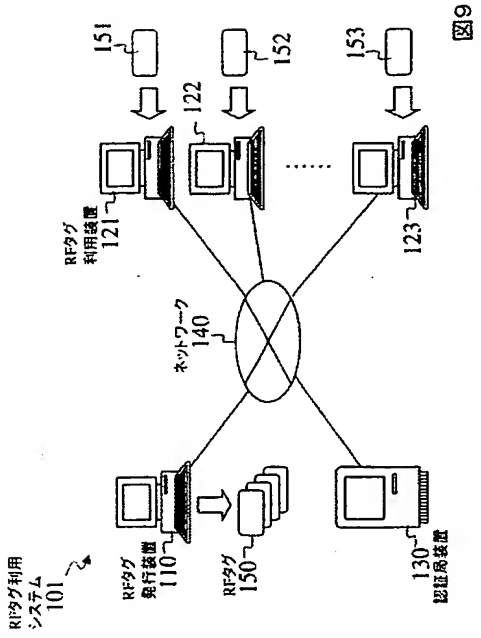


図9

【図１０】

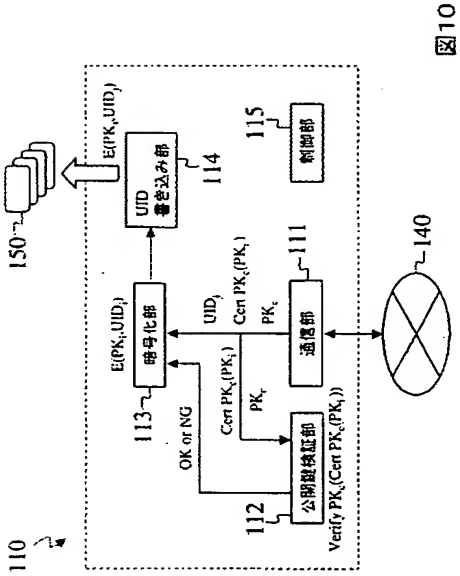


図10

【図１１】

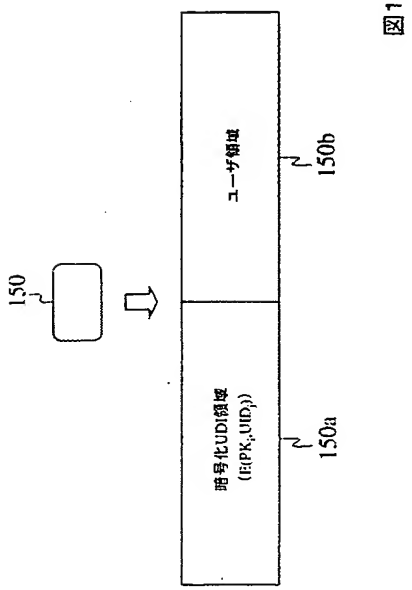


図11

【図１２】

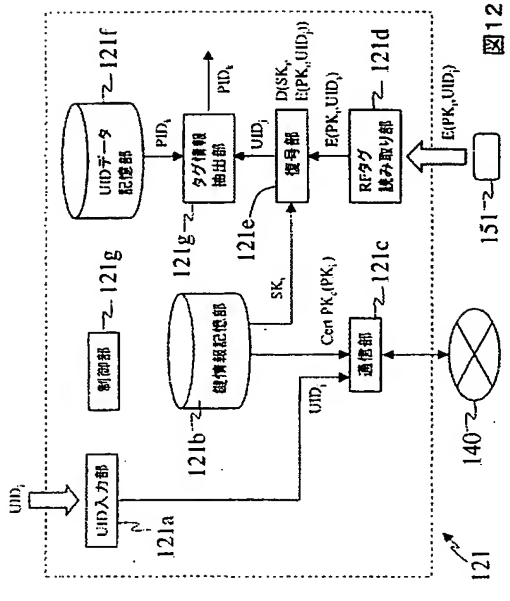


図12

【図１３】

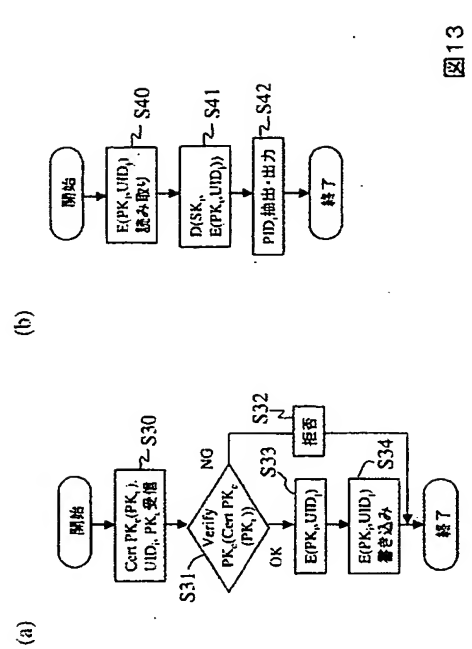


図13

【図１４】

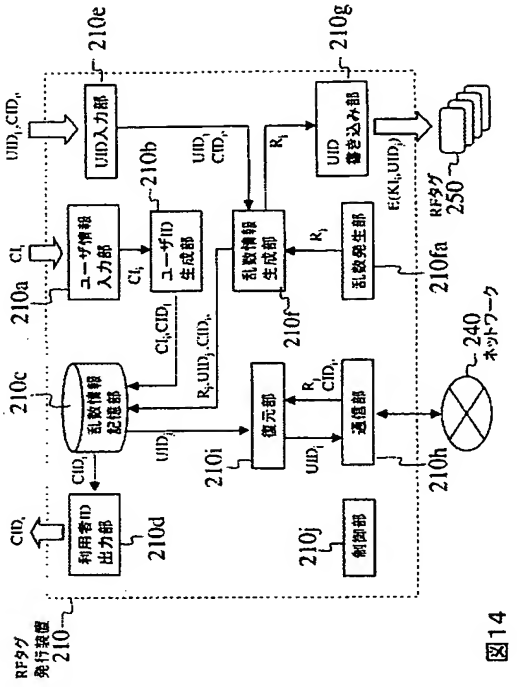


図14

【図１５】

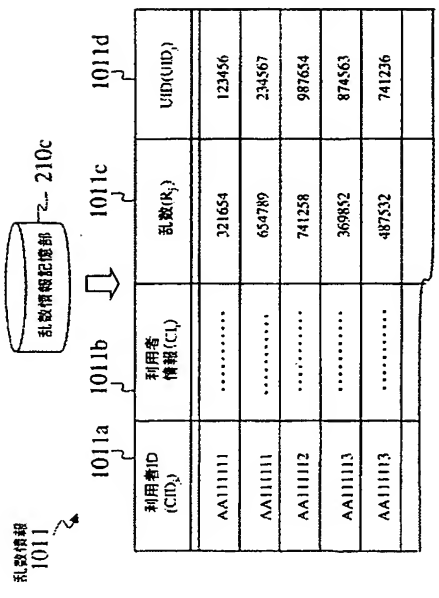


図15

【図１６】

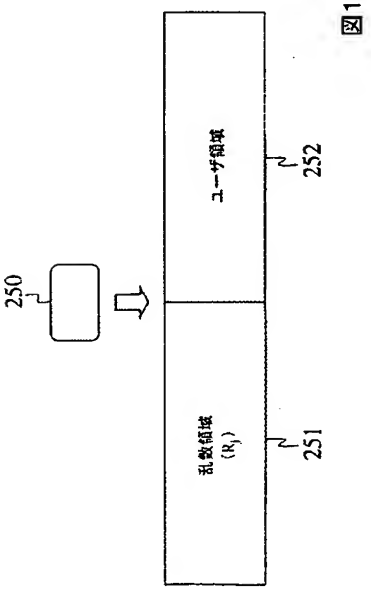


図16

【図１７】

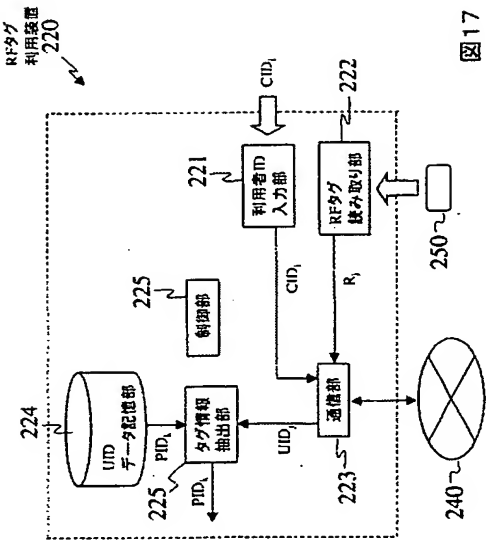


図17

【図１８】

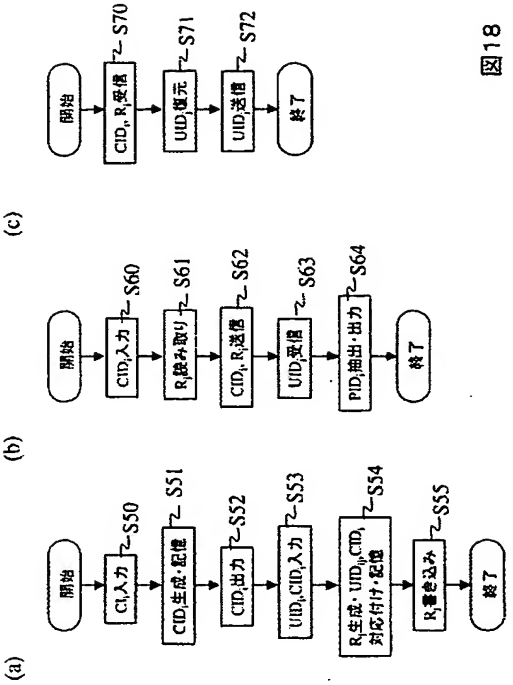


図18

【図１９】

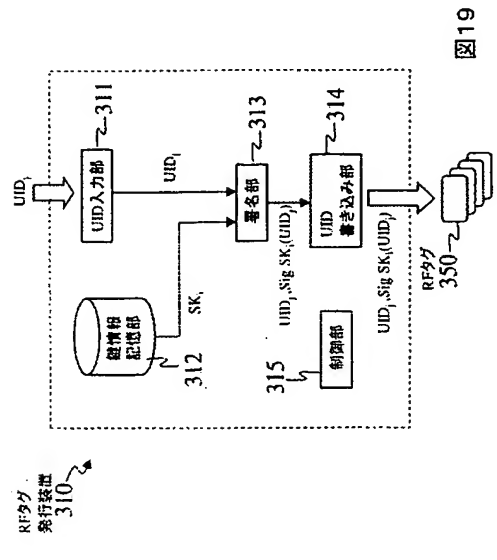


図19

【図２０】

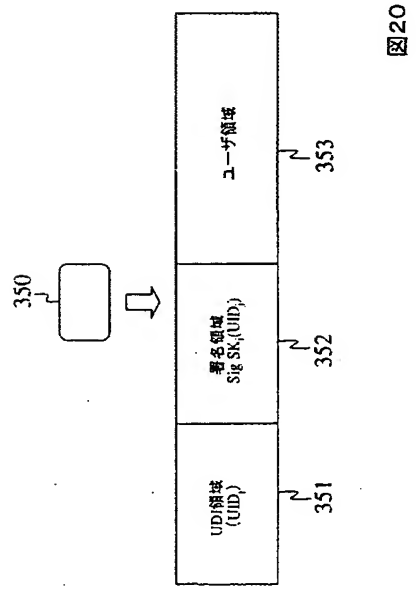


図20

【図２１】

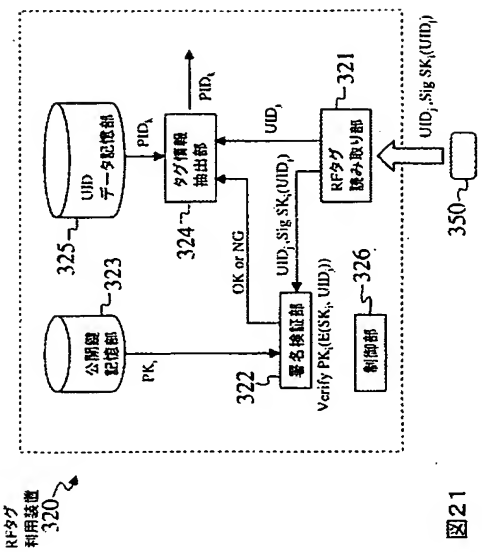


図21

【図２２】

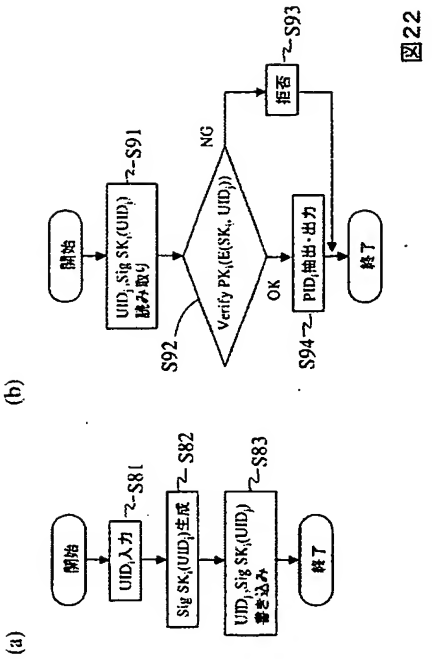


図22

【図２３】

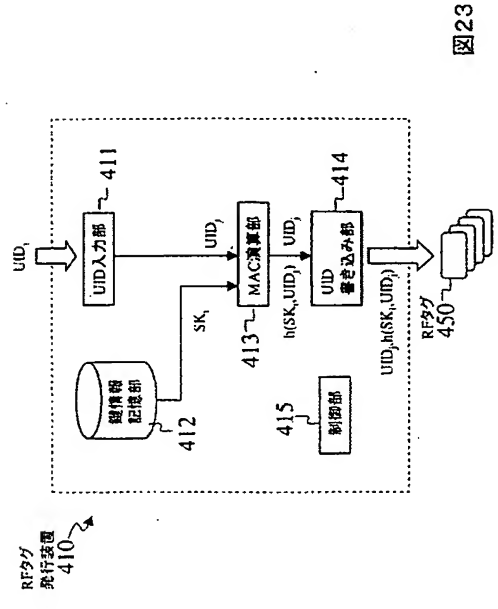


図23

【図２４】

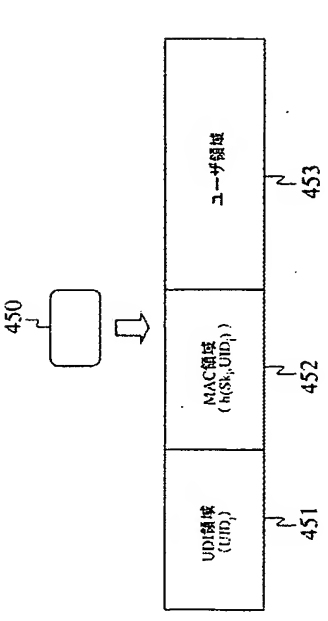


図24

【図２５】

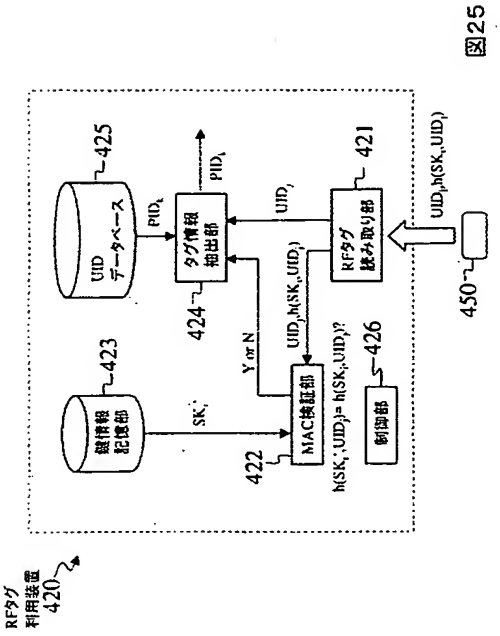


図25

【図２６】

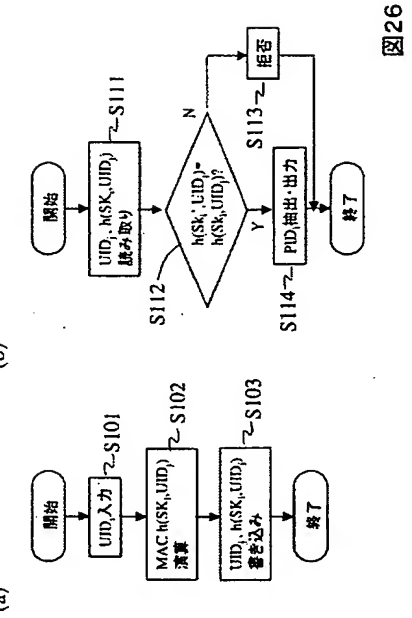


図26

【図２７】

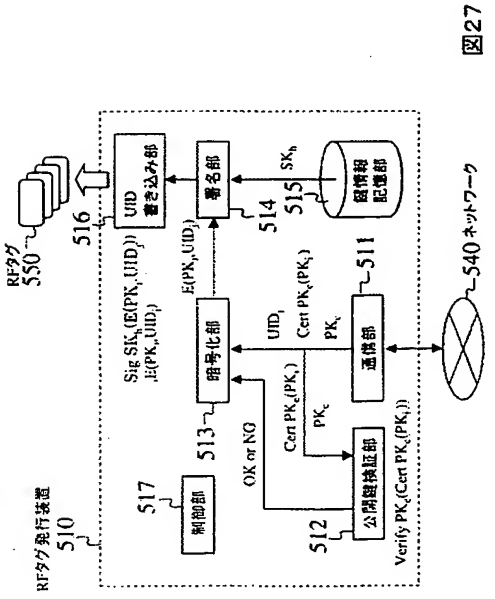


図27

【図２８】

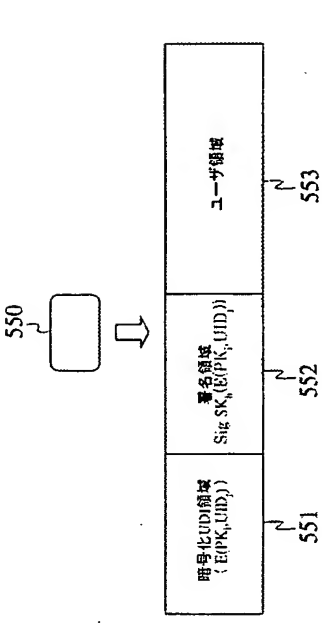


図28

【図２９】

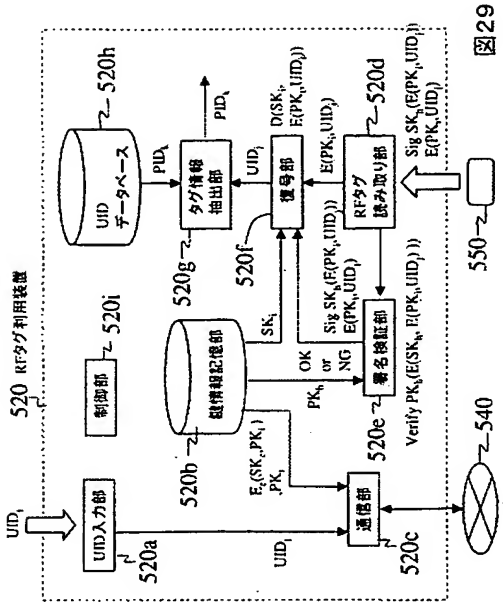


図29

【図３０】

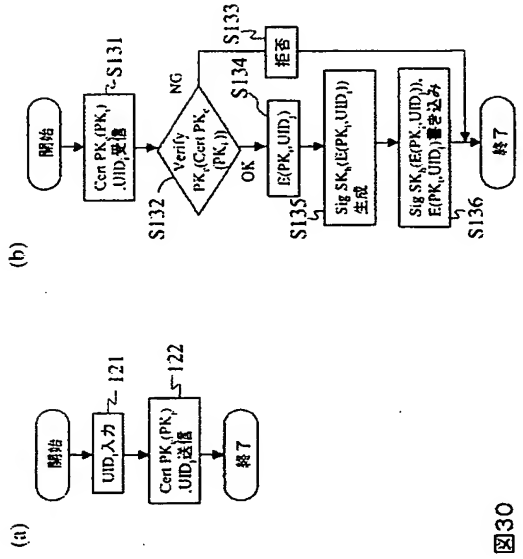


図30

【図３１】

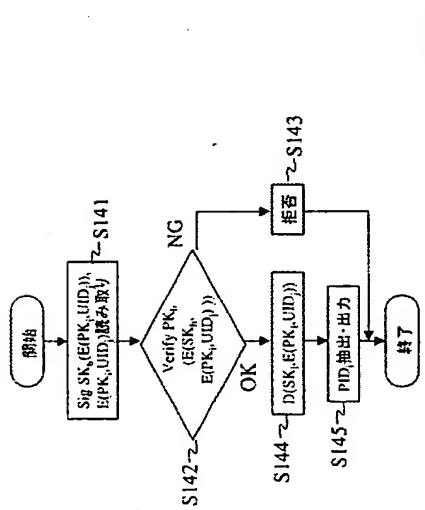


図31

【図３２】

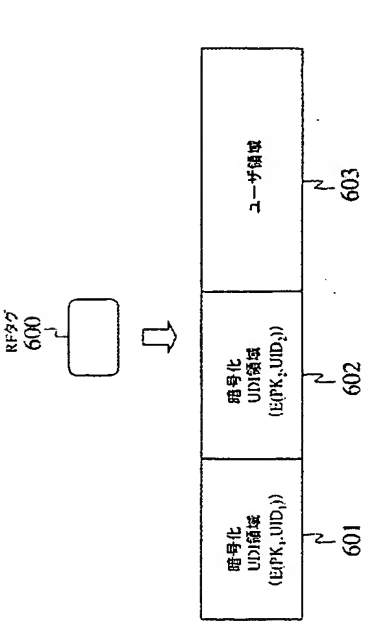


図32

【図３３】

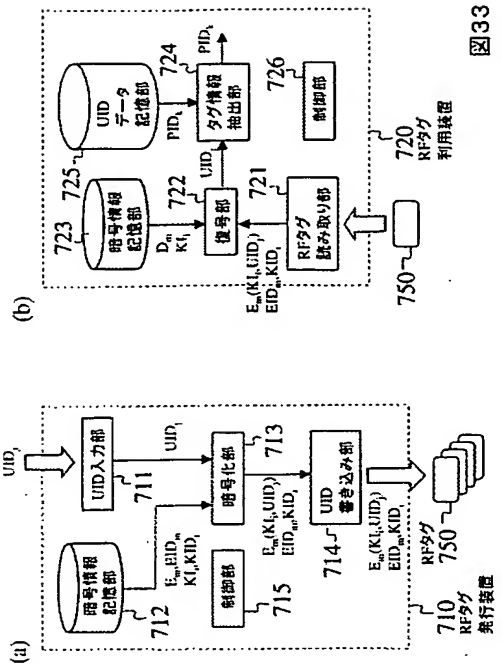


図33

【図３４】

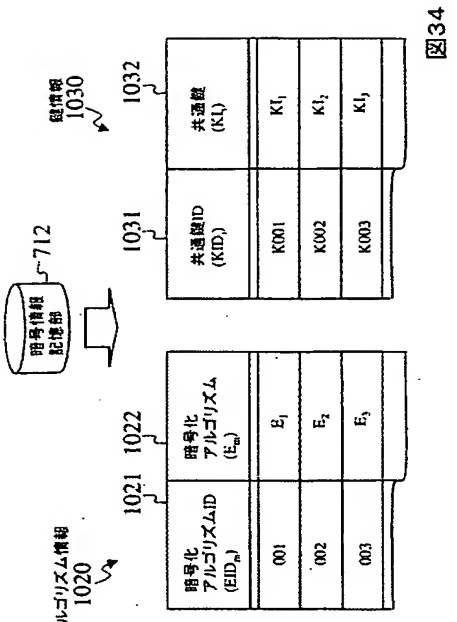


図34

【図３５】

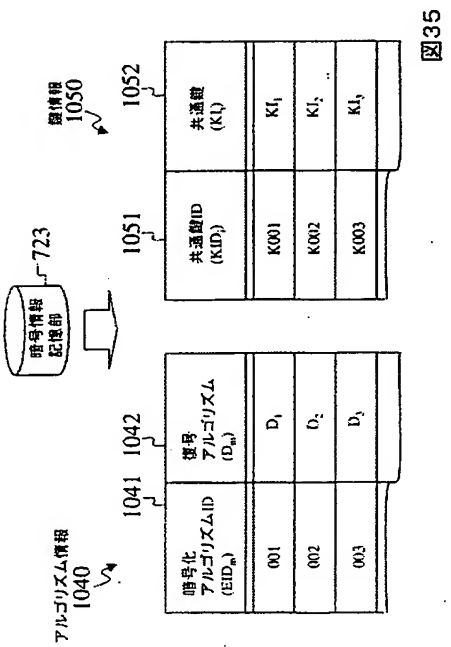


図35

【図３６】

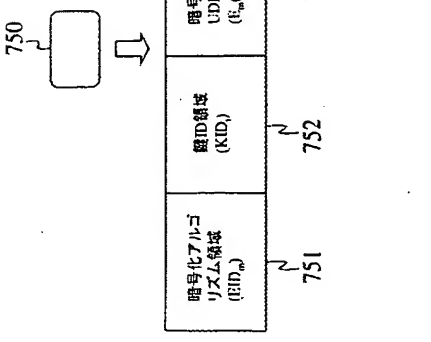


図36

【図３７】

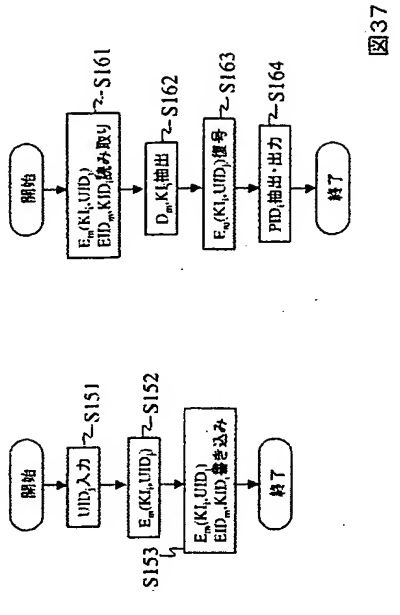


図37

【図３８】

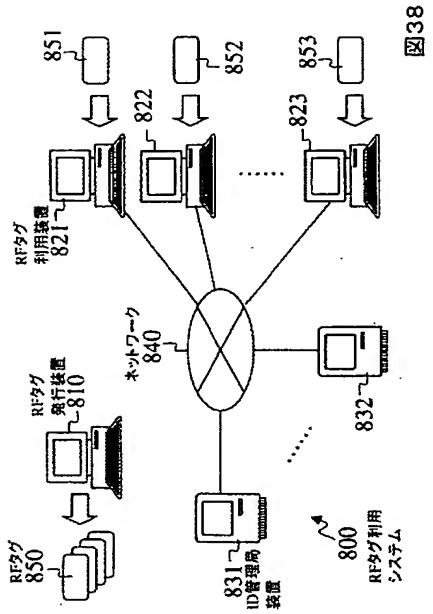


図38

【図３９】

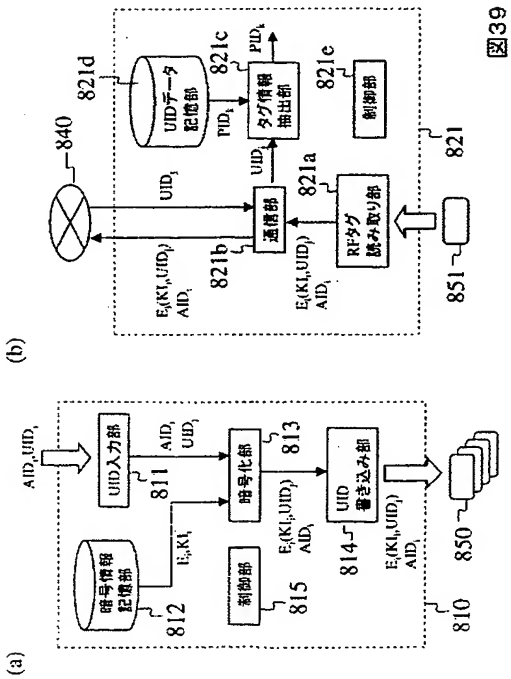


図39

【図４０】

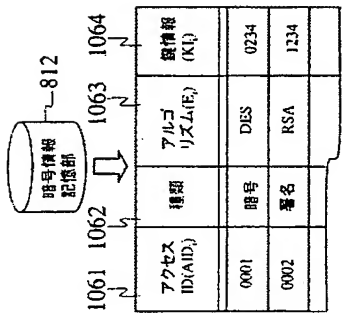


図40

【図４１】

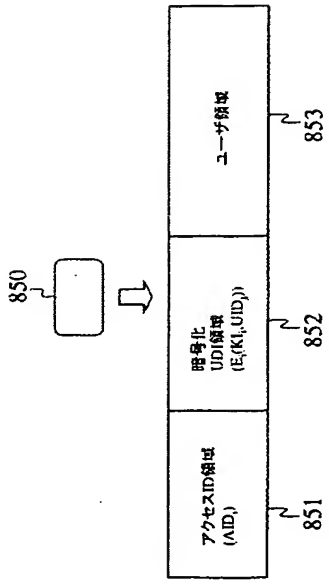


図41

【図４２】

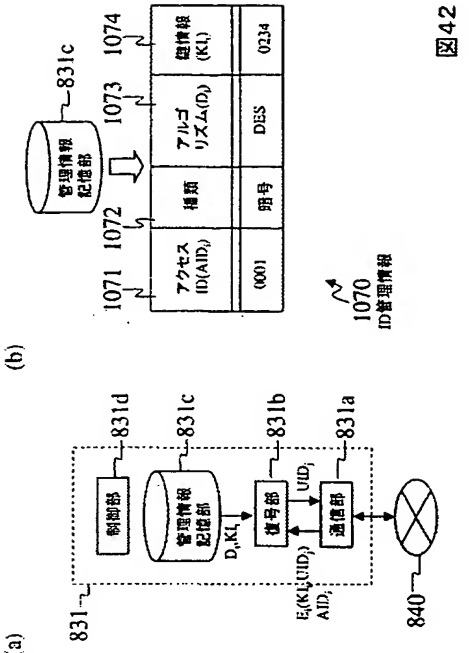


図42

【図４３】

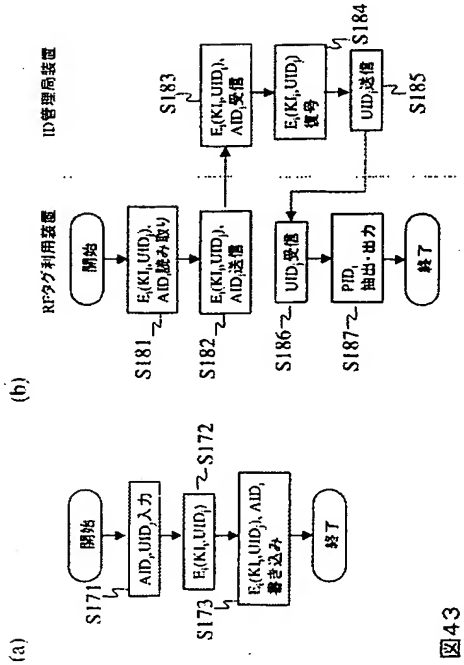


図43

フロントページの続き

(72)発明者 星野 文学
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内
(72)発明者 藤村 明子
東京都千代田区大手町二丁目３番１号 日本電信電話株式会社内

Ｆターム(参考) 5B058 CA15 CA25 KA01 KA04 KA11 KA31 KA32 KA35
5J104 AA07 NA36 PA10